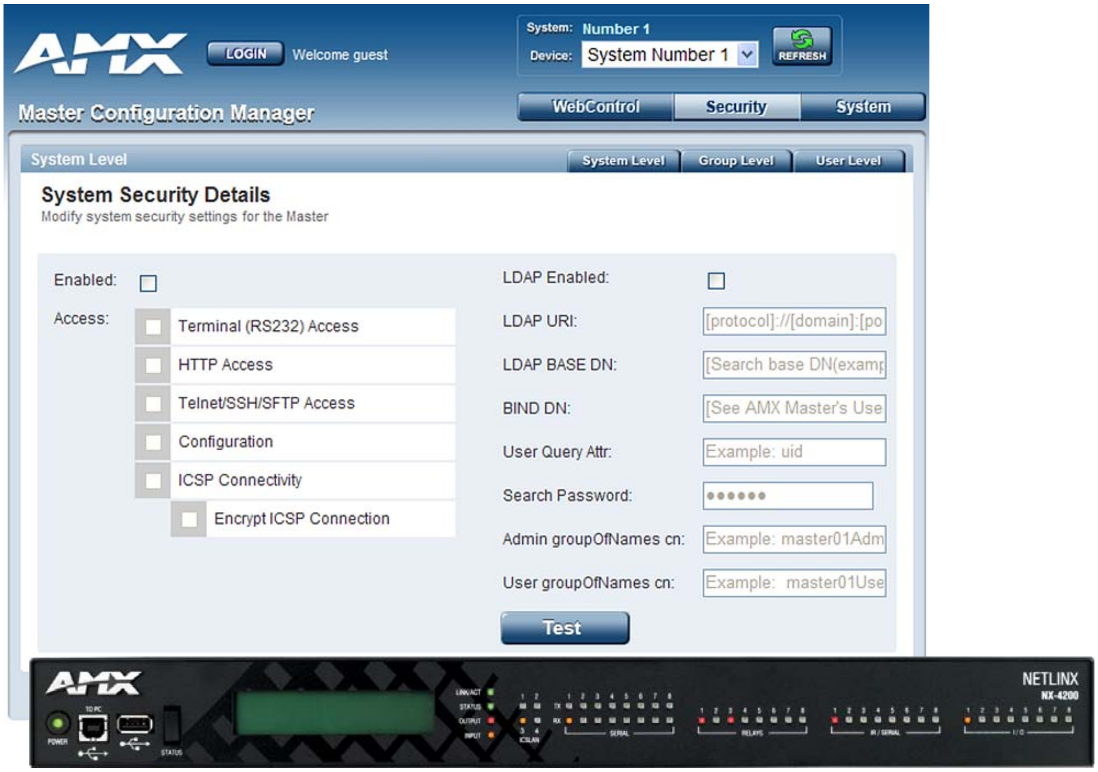
WebConsole & Programming Guide

NX-Series Controllers

NX-1200
NX-2200
NX-3200
NX-4200



System: Number 1
Device: System Number 1

System Security Details

Modify system security settings for the Master

Enabled: □

Access:
- □ Terminal (RS232) Access
- □ HTTP Access
- □ Telnet/SSH/SFTP Access
- □ Configuration
- □ ICSP Connectivity
  - □ Encrypt ICSP Connection

LDAP Enabled: □

LDAP URI: [protocol]://[domain]:[po

LDAP BASE DN: [Search base DN(examp

BIND DN: [See AMX Master's Use

User Query Attr: Example: uid

Search Password: ●●●●●●

Admin groupOfNames cn: Example: master01Adm

User groupOfNames cn: Example: master01Use

Central Controllers

Initial Release: 6/26/2014

AMX Limited Warranty and Disclaimer

This Limited Warranty and Disclaimer extends only to products purchased directly from AMX or an AMX Authorized Partner which include AMX Dealers, Distributors, VIP's or other AMX authorized entity.

AMX warrants its products to be free of defects in material and workmanship under normal use for three (3) years from the date of purchase, with the following exceptions:

- Electroluminescent and LCD Control Panels are warranted for three (3) years, except for the display and touch overlay components are warranted for a period of one (1) year.
- Disk drive mechanisms, pan/tilt heads, power supplies, and MX Series products are warranted for a period of one (1) year.
- AMX lighting products are guaranteed to switch on and off any load that is properly connected to our lighting products, as long as the AMX lighting products are under warranty. AMX also guarantees the control of dimmable loads that are properly connected to our lighting products. The dimming performance or quality there of is not guaranteed, impart due to the random combinations of dimmers, lamps and ballasts or transformers.
- AMX software is warranted for a period of ninety (90) days.
- Batteries and incandescent lamps are not covered under the warranty.
- AMX AutoPatch Epica, Modula, Modula Series4, Modula CatPro Series and 8Y-3000 product models will be free of defects in materials and manufacture at the time of sale and will remain in good working order for a period of three (3) years following the date of the original sales invoice from AMX. The three-year warranty period will be extended to the life of the product (Limited Lifetime Warranty) if the warranty card is filled out by the dealer and/or end user and returned to AMX so that AMX receives it within thirty (30) days of the installation of equipment but no later than six (6) months from original AMX sales invoice date. The life of the product extends until five (5) years after AMX ceases manufacturing the product model. The Limited Lifetime Warranty applies to products in their original installation only. If a product is moved to a different installation, the Limited Lifetime Warranty will no longer apply, and the product warranty will instead be the three (3) year Limited Warranty.

All products returned to AMX require a Return Material Authorization (RMA) number. The RMA number is obtained from the AMX RMA Department. The RMA number must be clearly marked on the outside of each box. The RMA is valid for a 30-day period. After the 30-day period the RMA will be cancelled. Any shipments received not consistent with the RMA, or after the RMA is cancelled, will be refused. AMX is not responsible for products returned without a valid RMA number.

AMX is not liable for any damages caused by its products or for the failure of its products to perform. This includes any lost profits, lost savings, incidental damages, or consequential damages. AMX is not liable for any claim made by a third party or by an AMX Authorized Partner for a third party.

This Limited Warranty does not apply to (a) any AMX product that has been modified, altered or repaired by an unauthorized agent or improperly transported, stored, installed, used, or maintained; (b) damage caused by acts of nature, including flood, erosion, or earthquake; (c) damage caused by a sustained low or high voltage situation or by a low or high voltage disturbance, including brownouts, sags, spikes, or power outages; or (d) damage caused by war, vandalism, theft, depletion, or obsolescence.

This limitation of liability applies whether damages are sought, or a claim is made, under this warranty or as a tort claim (including negligence and strict product liability), a contract claim, or any other claim. This limitation of liability cannot be waived or amended by any person. This limitation of liability will be effective even if AMX or an authorized representative of AMX has been advised of the possibility of any such damages. This limitation of liability, however, will not apply to claims for personal injury.

Some states do not allow a limitation of how long an implied warranty last. Some states do not allow the limitation or exclusion of incidental or consequential damages for consumer products. In such states, the limitation or exclusion of the Limited Warranty may not apply. This Limited Warranty gives the owner specific legal rights. The owner may also have other rights that vary from state to state. The owner is advised to consult applicable state laws for full determination of rights.

EXCEPT AS EXPRESSLY SET FORTH IN THIS WARRANTY, AMX MAKES NO OTHER WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. AMX EXPRESSLY DISCLAIMS ALL WARRANTIES NOT STATED IN THIS LIMITED WARRANTY. ANY IMPLIED WARRANTIES THAT MAY BE IMPOSED BY LAW ARE LIMITED TO THE TERMS OF THIS LIMITED WARRANTY. EXCEPT AS OTHERWISE LIMITED BY APPLICABLE LAW, AMX RESERVES THE RIGHT TO MODIFY OR DISCONTINUE DESIGNS, SPECIFICATIONS, WARRANTIES, PRICES, AND POLICIES WITHOUT NOTICE.

Table of Contents

Overview 1

NetLinx Integrated Controllers 1

About This Document 1

Quick Setup and Configuration Overview 2

Installation Procedures 2

Configuration and Communication 2

Update the On-board Master and Controller Firmware 2

Configure NetLinx Security on the NX Controller 2

Using Zero Configuration 3

Bonjour (Zero-Configuration) Client 3

Connecting to a Network with a DHCP Server 3

Initial Configuration 4

Overview 4

Before You Start 4

Preparing the NX Controller for USB Communication 4

Configuring the NX Controller for LAN Communication 6

Obtaining the NX Controller's IP Address (using DHCP) 8

Assigning a Static IP to the NX Controller 9

Communicating via IP Address 10

Upgrading Firmware 13

Overview 13

NX Controllers - Firmware Files 13

NX Master Firmware 13

Device Controller Firmware 13

Before You Start 14

Verifying the Current Firmware Version 14

Downloading the Latest Firmware Files from www.amx.com 15

NetLinx Integrated Controllers 15

Master and Device Firmware Kit Files for NX-Series Controllers 15

Downloading NX-Series Controller Firmware Files on www.amx.com 15

Required Order of Firmware Updates 15

Upgrading Firmware via USB 15

Upgrading Firmware via NetLinx Studio 16

Resetting the Factory Default System and Device Values 18

On-Board WebConsole User Interface 19

WebConsole UI Overview 19

Accessing the WebConsole 20

Default User Names and Passwords 20

Device Tree 20

Device Network Settings Pages 21

ZeroConfig Networking 21

WebConsole - Security Options 22

Security Overview 22

Default Security Configuration 23

Login Rules 23

User Name and Password Rules 23

System Security - System Level 24

System Level Security - System Security Settings 24

Access Options 24

LDAP Options 25

Configuring ICSP Connectivity with LDAP Enabled 26

Accepting Changes 26

Testing the Connection to the LDAP Server 26

System Security - Group Level 27

Adding a New Group 27

Group and User Security Access Options 28

Viewing Group Security Settings Details 29

Modifying the Properties of an Existing Group 29

Deleting a Group 30

System Security - User Level 30

Adding a New User 31

Viewing and Editing User Security Settings 32

Deleting a User 32

Wired 802.1X support 32

WebConsole - Web Control Options 33

Manage Web Control Connections 33

Compression Options 33

WebConsole - System Options 34

System Overview 34

System - Manage System 34

Manage System - System Number 35

Changing the System Number on the Master 35

Using Multiple NetLinx Masters 35

Resetting the Master Controller to the Factory Defaults Configuration 35

Manage System - Control/Emulate Options 36

Controlling or Emulating a System Device 37

Manage System - Diagnostics Options 39

Enabling Diagnostics on a Selected System Device 40
Diagnostics Options Definitions 43
Disabling all Diagnostic Options for a Device 43
Creating and Recalling Diagnostics Presets 44
Manage System - Server Options 44
Port Settings 45
Server Port Settings 45
SSL Certificate Options 46
Creating an SSL Server Certificate 47
SSL Certificate Entries 48
Displaying SSL Server Certificate Information 48
Creating a Request for an SSL Certificate 49
Self-Generating an SSL Certificate 49
Regenerating an SSL Server Certificate Request 49
Exporting an SSL Certificate Request 49
Importing an SSL Certificate 50
Manage System - Clock Manager Options 51
Setting the Mode for the Clock Manager 51
Setting Daylight Savings Rules 52
Selecting a Custom NIST Server 53
Adding a Custom NIST Server to the List 53
Clock Manager NetLinx Programming API 53
Manage System - App Manager Options 54
System - Manage License 54
Adding a New License 55
Removing a License 55
System - Manage NetLinx 56
System - Manage Devices 57
Manage Devices - Device Options 58
Configuring Device Binding Options 58
Managing Device Modules 58
Archiving a Module 58
Deleting a Module 59
Manage Devices - Bindings 59
Configuring Application-Defined Devices 59
Application Devices and Association Status 61
Viewing Physical Device Properties 62
Manage Devices - User-Defined Devices 62
Adding a User-Defined Device 63
Manage Devices - Active Devices 64
Searching For All Compatible Duet Modules for a Selected Device 64

Viewing Physical Device Properties 65
Manage Devices - Manage Polled Ports 66
Editing Polled Port Settings 66
Manage Devices - Network Settings 67
Manage Devices - URL List 68
Adding a URL to the Master's List of Devices 68
Manage Devices - Device Number 69
Manage Devices - Control/Emulate 69
Manage Devices - Log 70
Manage Devices - Diagnostics 71
NetLinx Programming 72
Overview 72
Port Assignments by NetLinx Master 72
Master SEND_COMMANDs 72
CLOCK 72
Master IP Local Port SEND_COMMANDs 73
UDPSENDTO 73
G4WC 73
~IGNOREEXTERNALCLOCKCOMMANDS 73
LED SEND_COMMANDs 74
LED-DIS 74
LED-EN 74
RS232/422/485 Ports Channels 74
RS-232/422/485 SEND_COMMANDs 74
B9MOFF 74
B9MON 75
CHARD 75
CHARDM 75
CLEAR FAULT 75
CTSPSH 75
CTSPSH OFF 75
GET BAUD 76
GET FAULT 76
GET STATUS 76
HSOFF 76
HSON 76
RXCLR 76
RXOFF 76
RXON 77
SET BAUD 77
SET FAULT DETECT OFF 77
SET FAULT DETECT ON 77
TSET BAUD 78
TXCLR 78
XOFF 78
XON 78

RS-232/422/485 SEND_STRING Escape Sequences 79
27,17,<time> 79
27,18,0 79
27,18,1 79
27,19,<time> 79
27,20,0 79
27,20,1 79
IR/Serial Ports Channels 80
IRRX Port Channels 80
IR/Serial SEND_COMMANDs 80
CAROFF 80
CARON 80
CH 81
CLEAR FAULT 81
CP 81
CTOF 81
CTON 81
GET BAUD 82
GET FAULT 82
GET MODE 82
GET STATUS 82
IROFF 82
POD 82
POF 83
PON 83
PTOF 83
PTON 83
SET BAUD 84
SET FAULT DETECT OFF 84
SET FAULT DETECT ON 84
SET IO LINK 84
SET MODE 84
SP 85
XCH 85
XCHM 86
Input/Output SEND_COMMANDs 87
GET DBT 87
SET DBT 87
GET INPUT 87
SET INPUT 87
PoE SEND_COMMANDs 88
GET CLASS 88
GET CURRENT 88
GET FAULT 88
GET STATUS 88
GET VOLTAGE 88
SET FAULT DETECT OFF 88
SET FAULT DETECT ON 88
SET POWER OFF 88
AxLink Commands 89
AXPWROFF 89

AXPWRON 89
GET AX FAULT 89
SET POWER ON 89
Terminal (Program Port/Telnet) Commands 90
Overview 90
Establishing a Terminal Connection via the Program Port 90
Establishing a Terminal Connection via Telnet 90
Terminal Commands 91
----- Help ----- <D:P:S> 91
? or Help 91
AUTO LOCATE (ENABLE|DISABLE|STATUS) 91
BOOT STATUS 91
CLEAR AUDIT LOG 91
CLEAR MAX BUFFERS 91
CLEAR PERSISTENT VARS 91
CPU USAGE 91
DATE 91
DATE/TIME ON|OFF 91
DEVICE HOLDOFF ON|OFF 91
DEVICE STATUS <D:P:S> 92
DIPSWITCH 92
DISK FREE 92
DNS LIST <D:P:S> 92
DOT1X (ENABLE|DISABLE|STATUS) 92
ECHO ON|OFF 92
EXPORT (CONFIG|CLONE) TO USB (FRONT|BACK) 93
GET DEVICE HOLDOFF 93
GET DUET MEMORY 93
GET ICSLAN 93
GET IP <D:P:S> 94
GET PLATFORM INFO 94
HELP SECURITY 94
ICSPMON ENABLED|DISABLED [PORT] 94
IMPORT CONFIG 94
IMPORT IRL 94
IMPORT KIT 94
IMPORT TKN 94
IP STATUS 94
MANAGE FIRMWARE 94
MEM 95
MSG ON|OFF 95
MSG STATS 95
NETLINX LOG LEVEL 95
OFF [D:P:S or NAME,CHAN] 95
ON [D:P:S or NAME,CHAN] 95
PASS [D:P:S or NAME] 96
PHYSICAL STATUS 96
PING [ADDRESS] 96
PROGRAM (ENABLE|DISABLE|STATUS) 96
PROGRAM INFO 96
PULSE [D:P:S or NAME,CHAN] 96

PWD 96
REBOOT 97
RENEW DHCP........ 97
RESETADMINPASSWORD 97
RESET FACTORY........ 97
ROUTE MODE DIRECT|NORMAL........ 97
SEND_COMMAND D:P:S or NAME,COMMAND 97
SEND_LEVEL <D:P:S>,<LEVEL ID>,<LEVEL VALUE> 97
SEND_STRING D:P:S or NAME,STRING........ 97
SET DATE 98
SET DNS <D:P:S> 98
SET DUET MEMORY 98
SET FTP PORT........ 98
SET HTTP PORT 98
SET HTTPS PORT 99
SET ICSLAN 99
SET ICSP PORT 99
SET ICSP TCP TIMEOUT........ 99
SET IP <D:P:S> 100
SET LOG COUNT 100
SET QUEUE SIZE........ 100
SET SECURITY PROFILE 101
SET SNMP........ 102
SET SSH PORT 102
SET SYSTEM NUMBER........ 103
SET TELNET PORT 103
SET THRESHOLD 103
SET TIME 103
SET TIMELINE LOOPCNT........ 103
SET UDP BC RATE 104
SET URL <D:P:S> 104
SHOW AUDIT LOG 104
SHOW BUFFERS 105
SHOW COMBINE........ 105
SHOW DEVICE <D:P:S>........ 105
SHOW LOG........ 106
SHOW MAX BUFFERS 107
SHOW MEM 107
SHOW NOTIFY 107
SHOW REMOTE........ 107
SHOW ROUTE 107
SHOW START LOG <START> 108
SHOW SYSTEM <S> 108
SHOW TCP 108
START LOG (ON|OFF)........ 108
TIME 108
URL LIST <D:P:S> 108

ESC Pass Codes........ 109

+ + ESC ESC 109
+ + ESC A 109
+ + ESC D 109
+ + ESC H 109
USB LOG [front|back] [enable|disable] 109

ZEROCONF[ENABLE|DISABLE|STATUS] 109
Accessing the Security Configuration Options........ 110
Setup Security Menu........ 111
Enabling LDAP via the Program Port 112
Security Options Menu........ 113
Edit User Menu 114
Edit Group Menu........ 114
Access Rights Menu 115
Adding a Group 115
Edit Group Menu: Add Directory Association 116
Default Security Configuration........ 117
Telnet Diagnostics Commands........ 118
PHYSICAL STATUS........ 118
MSG STATS 118
Logging Out of a Terminal Session 118
Notes on Specific Telnet/Terminal Clients 118
Windows Client Programs........ 118
Linux Telnet Client 118
Appendix A: LDAP Implementation Details 119
Overview 119
Assumptions and Prerequisites........ 119
AMX LDAP Client Authentication Sequence........ 119
Example - Setting Up User's Access Rights........ 121
Administrator Access Example 121
User Access Example 121
ICSP Connectivity Security Example........ 122
Appendix B: SMTP Support 123
Overview 123
SMTP Server Configuration 123
Sending Mail........ 124
Appendix C: Clock Manager NetLinx Programming API 125
Types/Constants 125
Library Calls 125
CLKMGR_IS_NETWORK_SOURCED()........ 125
CLKMGR_SET_CLK_SOURCE(CONSTANT INTEGER MODE) 125
CLKMGR_IS_DAYLIGHTSAVINGS_ON()........ 125
CLKMGR_SET_DAYLIGHTSAVINGS_MODE(CONSTANT INTEGER ONOFF) 125
CLKMGR_GET_TIMEZONE() 125
CLKMGR_SET_TIMEZONE(CONSTANT CHAR TIMEZONE[]) 125
CLKMGR_GET_RESYNC_PERIOD()........ 125
CLKMGR_SET_RESYNC_PERIOD(CONSTANT INTEGER PERIOD) 125
CLKMGR_GET_DAYLIGHTSAVINGS_OFFSET(CLKMGR_TIMEOFFSET_STRUCT T)........ 125

CLKMGR_SET_DAYLIGHTSAVINGS_OFFSET
(CONSTANT CLKMGR_TIMEOFFSET_STRUCT T) 125
CLKMGR_GET_ACTIVE_TIMESERVER(CLKMGR_TIMESERVER_STRUCT T) 125
CLKMGR_SET_ACTIVE_TIMESERVER(CONSTANT CHAR IP[]) 126
CLKMGR_GET_TIMESERVERS(CLKMGR_TIMESERVER_STRUCT T[])..................................... 126
CLKMGR_ADD_USERDEFINED_TIMESERVER
(CONSTANT CHAR IP[], CONSTANT CHAR URL[],
CONSTANT CHAR LOCATION[]) 126
CLKMGR_DELETE_USERDEFINED_TIMESERVER(CONSTANT CHAR IP[])............................. 126
CLKMGR_GET_START_DAYLIGHTSAVINGS_RULE() 126
CLKMGR_SET_START_DAYLIGHTSAVINGS_RULE(CONSTANT CHAR RECORD[]) 126
CLKMGR_GET_END_DAYLIGHTSAVINGS_RULE() 127
CLKMGR_SET_END_DAYLIGHTSAVINGS_RULE(CONSTANT CHAR RECORD[]) 127

Overview

NetLinx Integrated Controllers

NetLinx Integrated Controllers (Masters) can be programmed to control RS-232/422/485, Relay, IR/Serial, and Input/Output devices using the NetLinx Studio application (version 4.0 or higher).

NetLinx Integrated Controllers	
Name	Description
NX-1200	NetLinx Integrated Controller
NX-2200	NetLinx Integrated Controller
NX-3200	NetLinx Integrated Controller
NX-4200	NetLinx Integrated Controller

Note: *Refer to the Products > Central Controllers > NetLinx Integrated Controllers page at www.amx.com for details and variations available for these products.*

NX controllers feature an on-board Web Console which allows you to connect to the NX controller via a web browser and make various configuration and security settings. The WebConsole is described in this document (starting with the *On-Board WebConsole User Interface* section on page 19).

NX controllers are Duet-compatible and can be upgraded via firmware. Duet is a dual-interpreter firmware platform from AMX which combines the proven reliability and power of NetLinx with the extensive capabilities of the *Java*® *MicroEdition (Java Standard Edition Embedded)* platform. Duet simplifies the programming of a system that includes the NX controller and other third party devices by standardizing device and function definitions, defaulting touch panel button assignments, and controlling feedback methods.

Dynamic Device Discovery makes integration even easier by automatically identifying and communicating with devices which support this beaconing technology. Refer to the *Manage Devices - Device Options* section on page 58 for more detailed information on the use of *Dynamic Device Discovery* (DDD).

About This Document

This document describes using the on-board WebConsole, as well as NetLinx send commands and terminal communications to configure the NX controllers:

- Each major section of the WebConsole is described in a separate section of this document. Refer to:
  - the *On-Board WebConsole User Interface* section on page 19,
  - the *WebConsole - Web Control Options* section on page 33,
  - the *WebConsole - Security Options* section on page 22, and
  - the *WebConsole - System Options* section on page 34).
- The *Initial Configuration and Firmware Upgrade* section on page 5 describes upgrading the firmware on NX controllers.
- The *NetLinx Programming* section on page 72 lists and defines the NetLinx send commands that are supported by the NX controllers.
- The *Terminal (Program Port/Telnet) Commands* section on page 90 describes the commands and options available via a Telnet terminal session with the NX controller.

Quick Setup and Configuration Overview

Installation Procedures

The general steps involved with most common installations of this device include:

- Unpack and confirm the contents of box (see the *Specifications* tables in the *Hardware Reference Guide* for each controller).
- Connect all rear panel components and supply power to the NX controller from the external power supply.

Configuration and Communication

The general steps involved with setting up and communicating with the NX controllers' on-board Master. In the initial communication process:

- Set the boot-time operations on the rear Configuration DIP switch.
- Connect and communicate with the on-board Master via the Program port.
- Set the System Value being used with the on-board Master.
- Re-assign any Device values.
- Retrieve the DHCP Address for the on-board Master or assign a Static IP to the on-board Master.
- Once the IP information is determined, re-work the parameters for Master Communication to connect to the on-board Master via the LAN and not the Program port.

Update the On-board Master and Controller Firmware

- Before using your new NX controller, you must first update your NetLinx Studio to the most recent release.
- Upgrade the Integrated Controller firmware through an IP address via the LAN connector (*Upgrading the NI Controller Firmware* section on page 21) (**IP recommended**).
- Upgrade the on-board Master firmware through an IP address via the LAN connector (*Upgrading Firmware* section on page 18) (**IP recommended**).

Configure NetLinx Security on the NX Controller

- Setup and finalize your NetLinx Security Protocols (*WebConsole - Security Options* section on page 22).
- Program your NX controller (*NetLinx Programming* section on page 72).

Using Zero Configuration

NetLinx Masters support using "zero-configuration" client software to quickly install multiple devices on the network.

Bonjour (Zero-Configuration) Client

You can use a zero-configuration client to determine the IP address of the Controllers. There are many zero-configuration clients available which are free and widely available for download. NetLinx Studio includes a zero-configuration client which we will use for the purposes of this document.

If you don’t already have it installed on your PC, download and install NetLinx Studio 4.0 before you begin.

Connecting to a Network with a DHCP Server

By using the Controller’s Zeroconf feature and the NetLinx Studio, you can install and configure multiple devices on the network without pre-configuring each device before installation.

The dealer only needs to match the serial number printed on the backside of the device or from the label on the box to the serial number that is displayed in the Bonjour browser pane.

1. Launch NetLinx Studio 4.0.
2. Once power is applied to the device, select the Zero-Config tab on the Workspace bar (see FIG. 1).

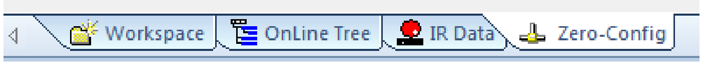
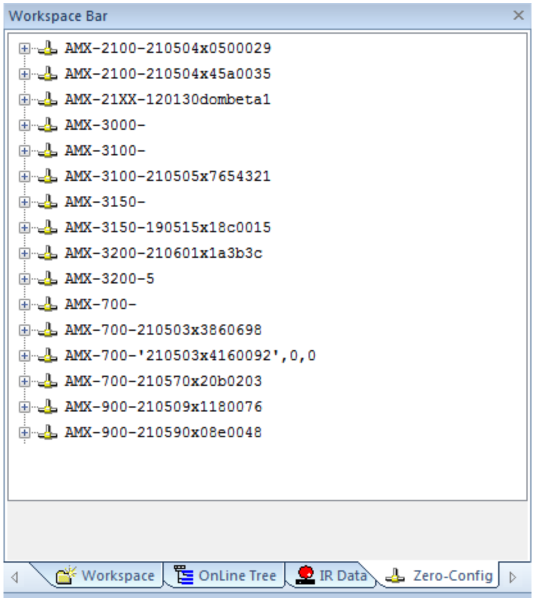


FIG. 1 Zero-Config tab

3. In the Workspace area, right-click and select **Refresh Zero Config List**. The controller appears in the list of devices as shown in FIG. 2:



```
AMX-2100-210504x0500029
AMX-2100-210504x45a0035
AMX-21XX-120130dombeta1
AMX-3000-
AMX-3100-
AMX-3100-210505x7654321
AMX-3150-
AMX-3150-190515x18c0015
AMX-3200-210601x1a3b3c
AMX-3200-5
AMX-700-
AMX-700-210503x3860698
AMX-700-'210503x4160092',0,0
AMX-700-210570x20b0203
AMX-900-210509x1180076
AMX-900-210590x08e0048
```

FIG. 2 Workspace bar (Zero-Config tab selected)

4. Double-click the Master you want to access it in the WebConsole.

   Accessing the Master requires valid login information. The browser will prompt you for User ID and Password before displaying the configuration pages for the selected device.

   Note that the serial number is appended to the name of the device.

After logging in, you can configure the device (changing IP settings, NetLinx settings, User settings, etc) via the pages in the WebConsole (see the *On-Board WebConsole User Interface* section on page 19).

Initial Configuration

Overview

This section describes using the NetLinx Studio software application to perform the initial configuration of the NetLinx Master. NetLinx Studio is used to setup a System number, obtain/assign the IP/URL for the NX controller, as described in this section (as well as to transfer firmware Kit files to the Master - see the *Upgrading Firmware* section on page 13).

Before You Start

1. Verify you have the latest version of the NetLinx Studio application version 4.0 installed on your PC.

   NetLinx Studio is available to download from **www.amx.com**. Login to download the latest version. Alternatively, if it is already installed, use the **Web Update** option in NetLinx Studio's Help menu to obtain the latest version.

   The default location for the NetLinx Studio application is **Start** > **Programs** > **AMX Control Disc** > **NetLinx Studio** > **NetLinx Studio**.
2. Verify that an LAN cable is connected from the NX controller to the LAN Hub.
3. Connect a programming cable (Type-B USB) from the **Program Port** on the NX controller to a USB port on the PC being used for programming.
4. Apply power to the NX controller.

Preparing the NX Controller for USB Communication

To establish USB communication with the NX controller via the PROGRAM port with Type-B-to-Type-A cable:

1. Launch NetLinx Studio and select **Settings** > **Workspace Communication Settings** (FIG. 3):

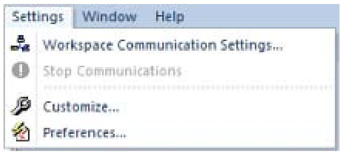


FIG. 3 NetLinx Studio menu bar - Settings > Workspace Communication Settings

2. This opens the *Workspace Communication Settings* dialog (FIG. 4).

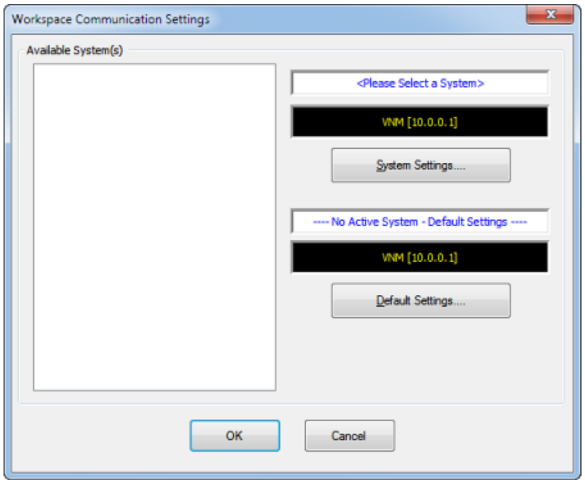
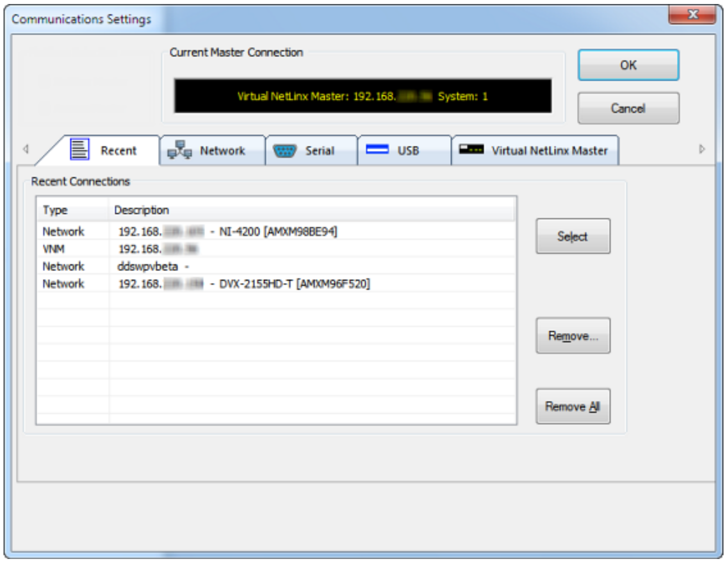


FIG. 4 Workspace Communication Settings dialog

3. Click the **System Settings** button to open the *Communications Settings* dialog (FIG. 5). If there is no system selected, click the **Default Settings** button to open the dialog.



Current Master Connection

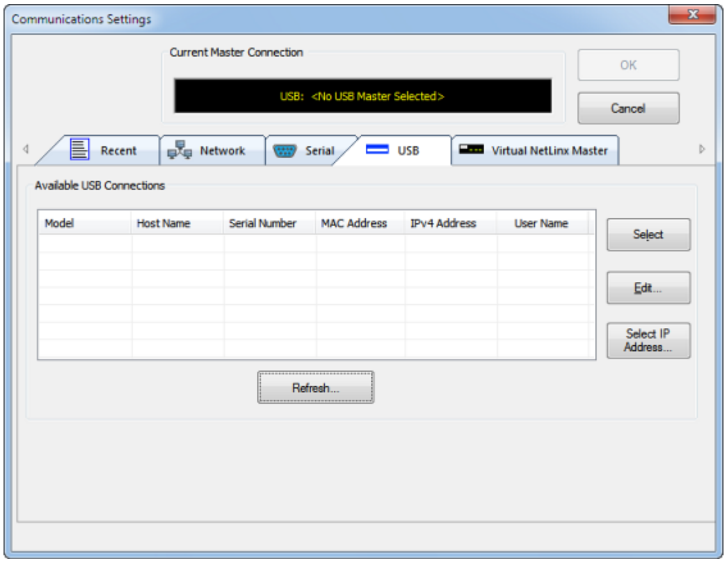
Virtual NetLinx Master: 192.168.[redacted] System: 1

Recent Connections

Type	Description
Network	192.168.[redacted] - NI-4200 [AMXM98BE94]
VNM	192.168.[redacted]
Network	ddswpvbeta -
Network	192.168.[redacted] - DVX-2155HD-T [AMXM96F520]

FIG. 5 Communication Settings dialog - Recent tab

4. Select the **USB** tab to view the USB options (FIG. 6).



Current Master Connection

USB: <No USB Master Selected>

Available USB Connections

Model	Host Name	Serial Number	MAC Address	IPv4 Address	User Name

FIG. 6 Communications Settings dialog - USB tab

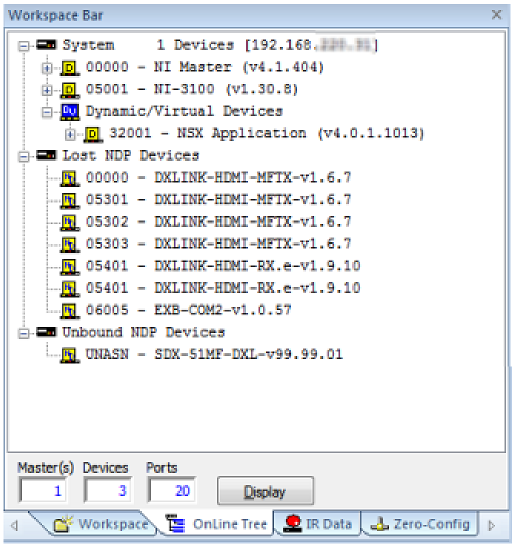
5. On the USB tab, highlight the Master you want to connect to and click **Select**.

6. Click **Edit** to open the Edit USB Master's Username/Password dialog to set the user name and password for authentication access to the Master. This step is optional. You can only change the user name and password in the dialog. The additional fields are view-only.

7. Click **OK** to close the USB Master's Username/Password dialog, and click **OK** in the Communication Settings dialog to return to the Communication Settings dialog, now indicating the USB-connected Master as the current connection configuration.

8. Click **OK** to close the *Communication Settings* dialog and return to the main application.

9. Right-click the **Online Tree** tab entry and select **Refresh System:** the Controller should appear in the Device Tree (FIG. 7):



```
System      1 Devices [192.168.[redacted]]
  00000 - NI Master (v4.1.404)
  05001 - NI-3100 (v1.30.8)
  Dynamic/Virtual Devices
    32001 - NSX Application (v4.0.1.1013)
Lost NDP Devices
  00000 - DXLINK-HDMI-MFTX-v1.6.7
  05301 - DXLINK-HDMI-MFTX-v1.6.7
  05302 - DXLINK-HDMI-MFTX-v1.6.7
  05303 - DXLINK-HDMI-MFTX-v1.6.7
  05401 - DXLINK-HDMI-RX.e-v1.9.10
  05401 - DXLINK-HDMI-RX.e-v1.9.10
  06005 - EXB-COM2-v1.0.57
Unbound NDP Devices
  UNASN - SDX-51MF-DXL-v99.99.01
```

Master(s): 1 Devices: 3 Ports: 20

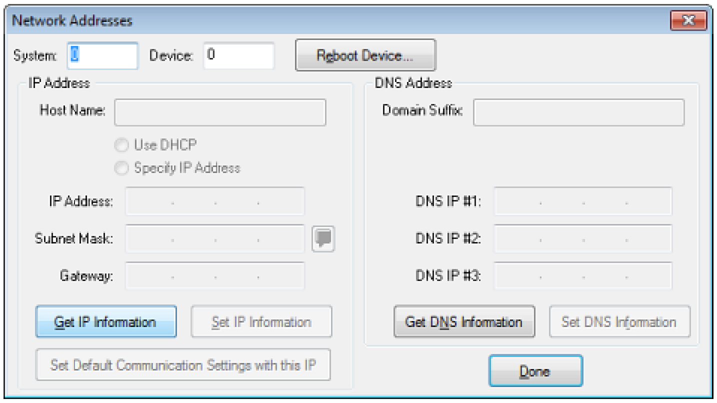
FIG. 7 Workspace Bar - Online Tree

If the Master does not appear in the list, verify that the USB cable is connected properly.

Once USB communication has been established, use NetLinx Studio to configure the Controller for LAN Communication, as described in the next section.

Configuring the NX Controller for LAN Communication

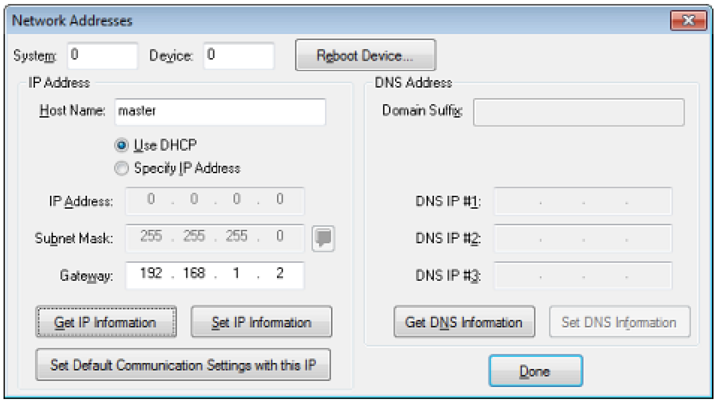
1. Use a LAN cable to connect the Controller to the LAN to which the PC running NetLinx Studio is connected.
2. Select **Diagnostics** > **Network Addresses** from the menu bar to open the *Network Addresses* dialog (FIG. 8). Use the options in this dialog to select to either use DHCP or specify an IP address.



System: 1 Device: 0

FIG. 8 Network Addresses dialog

3. Click **Get IP Information** to enable the fields for editing (FIG. 9):



Network Addresses

System: 0 Device: 0

IP Address

Host Name: master

● Use DHCP
○ Specify IP Address

IP Address: 0 . 0 . 0 . 0

Subnet Mask: 255 . 255 . 255 . 0

Gateway: 192 . 168 . 1 . 2

DNS Address

Domain Suffix:

DNS IP #1:

DNS IP #2:

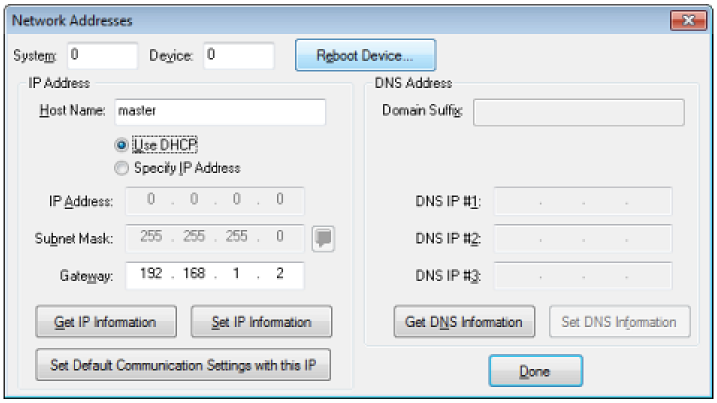
DNS IP #3:

FIG. 9 Network Addresses dialog showing initial IP information

4. Enter the *System*, *Device* (**0** for NetLinx Masters), and *Host Name* information.

Note: *Host names may contain only the ASCII letters 'a' through 'z' (in a case-insensitive manner), the digits '0' through '9', and the hyphen ('-').*

5. To configure a network address via **DHCP** (FIG. 10):



Network Addresses

System: 0 Device: 0

IP Address

Host Name: master

● Use DHCP
○ Specify IP Address

IP Address: 0 . 0 . 0 . 0

Subnet Mask: 255 . 255 . 255 . 0

Gateway: 192 . 168 . 1 . 2

DNS Address

Domain Suffix:

DNS IP #1:

DNS IP #2:

DNS IP #3:

FIG. 10 Network Addresses dialog (DHCP)

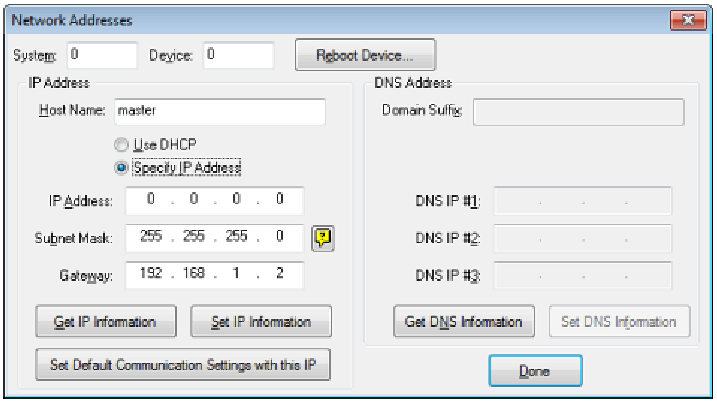
a. Select **Use DHCP**.

b. Click **Set IP Information** to retain the DHCP setting.

c. To finish the process, click **Reboot Device.**

d. Click **Done** to close the dialog.

6. To specify a network IP address (FIG. 11):



Network Addresses

System: 0 Device: 0

IP Address

Host Name: master

○ Use DHCP
● Specify IP Address

IP Address: 0 . 0 . 0 . 0

Subnet Mask: 255 . 255 . 255 . 0

Gateway: 192 . 168 . 1 . 2

DNS Address

Domain Suffix:

DNS IP #1:

DNS IP #2:

DNS IP #3:

FIG. 11 Network Addresses dialog (Specify IP Address)

a. Select **Specify IP Address.**

b. Enter the IP parameters into the available fields.

c. Click **Set IP Information** to retain the pre-reserved IP address to the Master.

d. To finish the process, click **Reboot Device.**

e. Click **OK** to close the dialog.

7. Repeat steps 1 - 5 from the previous section, but rather than selecting the **USB** tab, select **Network** and edit the settings to match the IP address you are using (Static or Dynamic).

8. If you want the Master to require authentication for access, enter a User Name and Password in the provided fields to secure the Master.

9. Click the **OK** to close all dialogs and return to the main application.

Obtaining the NX Controller's IP Address (using DHCP)

Note: *Verify there is an active LAN connection on the NX controller's LAN port before beginning these procedures.*

1. In NetLinx Studio, select **Diagnostics** > **Network Addresses** from the Main menu to access the Network Addresses dialog (FIG. 12).

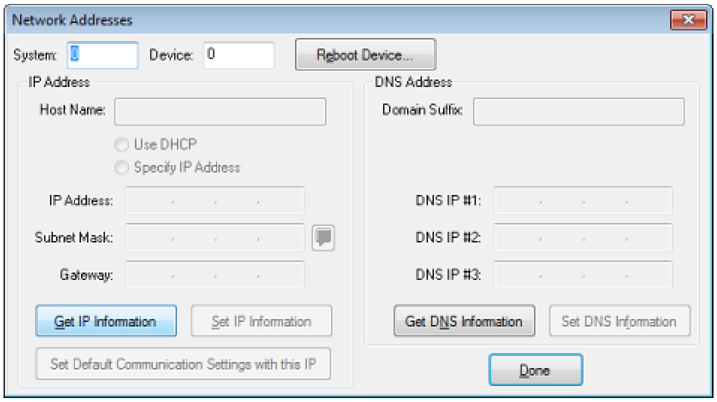


FIG. 12 NetLinx Studio: Network Addresses dialog

2. Verify that both the **System** number corresponds to the System value previously assigned within the Device Addressing tab and that zero (0) is entered into the *Device* field.

Note: *The system value must correspond to the Device Address entered in the Device Addressing dialog. Refer to the Manage System - System Number section on page 46 for more detailed instructions on setting a system value.*

3. Click **Get IP Information** to enable the Use DHCP and Specify IP Address options.

4. Select **Use DHCP**.

Note: *DO NOT enter ANY IP information at this time; this step only gets the System Master to recognize that it should begin using an obtained DHCP Address.*

5. Click **Reboot Device**.

6. After the device has booted, repeat steps 1-3.

7. Note the obtained IP address (*read-only*). This information is later entered into the *Communication Settings* dialog and used by NetLinx Studio to communicate to the NX controller via an IP. This address is reserved by the DHCP server and then given to the Master.

Note: *If the IP Address field is empty, give the Master a few minutes to negotiate a DHCP Address with the DHCP Server, and try again. The DHCP Server can take anywhere from a few seconds to a few minutes to provide the Master with an IP address.*

Note: *Verify that these IP values are also entered into the related fields within either the IP Settings section of the System Connection page (on the touch panel) or within the Address field on the web browser.*

8. Click **Done** to close the dialog.

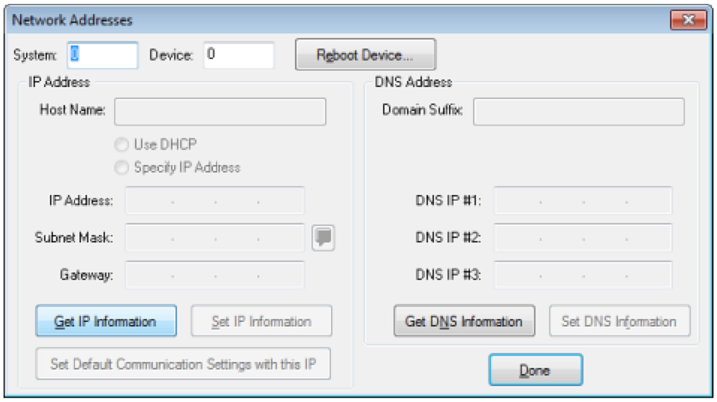
Note: *On the front panel of the NetLinx Master, the STATUS and OUTPUT LEDs should begin to alternately blink during the incorporation. Wait until the STATUS LED is the only LED to blink.*

Complete the communication process by continuing on to the *Communicating via IP Address* section on page 10.

Assigning a Static IP to the NX Controller

***Note:** Verify there is an active LAN connection on the LAN port of the Master before beginning these procedures.*

1. In NetLinx Studio, select **Diagnostics** > **Network Addresses** to open the *Network Addresses* dialog (FIG. 13):



Network Addresses

System: 0 Device: 0

IP Address

Host Name:

○ Use DHCP

○ Specify IP Address

IP Address:

Subnet Mask:

Gateway:

DNS Address

Domain Suffix:

DNS IP #1:

DNS IP #2:

DNS IP #3:

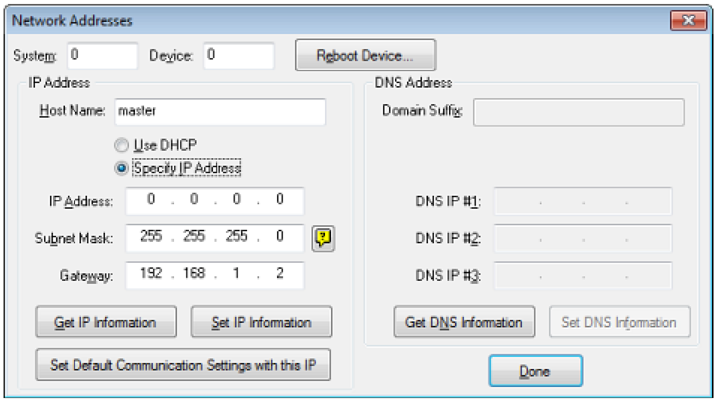
FIG. 13 NetLinx Studio: Network Addresses dialog

2. Verify that both the **System** number corresponds to the System value previously assigned within the Device Addressing tab and that zero (0) is entered into the *Device* field.

***Note:** The system value must correspond to the Device Address previously entered in the Device Addressing tab. Refer to the Manage System - System Number section on page 46 for more detailed instructions on setting a system value.*

3. Click the **Get IP Information** button to enable the *Use DHCP* and *Specify IP Address* options.

4. Select **Specify IP Address** to enable the IP fields for editing (FIG. 14):



Network Addresses

System: 0 Device: 0

IP Address

Host Name: master

○ Use DHCP

● Specify IP Address

IP Address: 0 . 0 . 0 . 0

Subnet Mask: 255 . 255 . 255 . 0

Gateway: 192 . 168 . 1 . 2

DNS Address

Domain Suffix:

DNS IP #1:

DNS IP #2:

DNS IP #3:

FIG. 14 NetLinx Studio: Network Addresses dialog (Specify IP Address)

5. Enter the *IP Address*, *Subnet Mask*, and *Gateway* information into their respective fields (as defined by the System Administrator).

***Note:** Verify that these IP values are also entered into the related fields within either the IP Settings section of the System Connection page (on the touch panel) or within the Address field on the web browser.*

6. Click **Set IP Information** to cause the on-board Master to retain this new IP address.

7. Click **Reboot Master**.

8. Click **Done** to close the dialog.

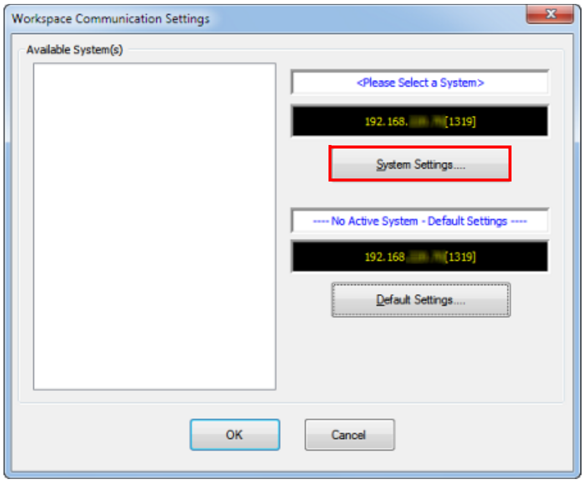
***Note:** On the front panel of the NetLinx Master, the STATUS and OUTPUT LEDs should begin to alternately blink during the incorporation. Wait until the STATUS LED is the only LED to blink.*

Complete the communication process by continuing on to the *Communicating via IP Address* section on page 10.

Communicating via IP Address

Whether the on-board Master’s IP address was set or obtained via DHCP, use the IP address information from the *Network Addresses* dialog to establish communication via the LAN-connected Master.

1. Use NetLinx Studio to obtain the IP address of the NX controller. If you do not have an IP address, follow the steps outlined in either the *Obtaining the NX Controller’s IP Address (using DHCP)* section on page 8, or the *Assigning a Static IP to the NX Controller* section on page 9.
2. Select **Settings** > **Workspace Communication Settings** from the Main menu to open the *Workspace Communication Settings* dialog (FIG. 15):



Workspace Communication Settings

Available System(s)

<Please Select a System>

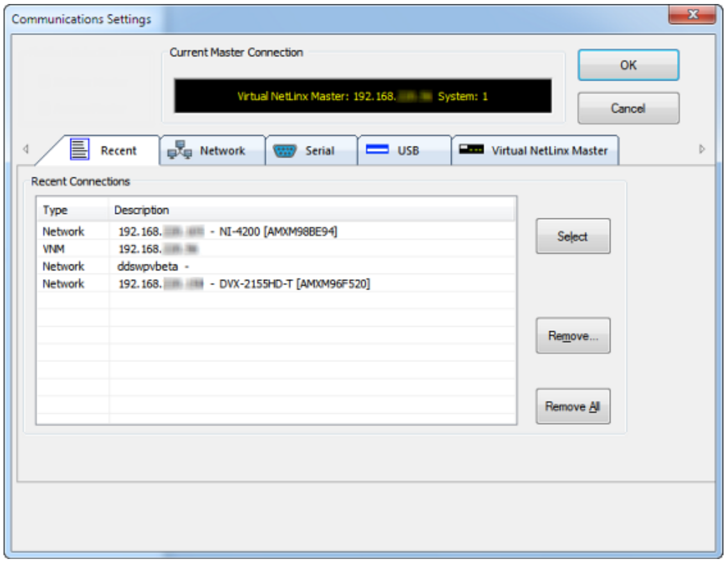
192.168.[redacted][1319]

---- No Active System - Default Settings ----

192.168[redacted][1319]

FIG. 15 NetLinx Studio - Workspace Communication Settings dialog

3. Click **System Settings** to open the *Communications Settings* dialog. If you do not have a system selected, click the **Default Settings** button (FIG. 16).



Communications Settings

Current Master Connection

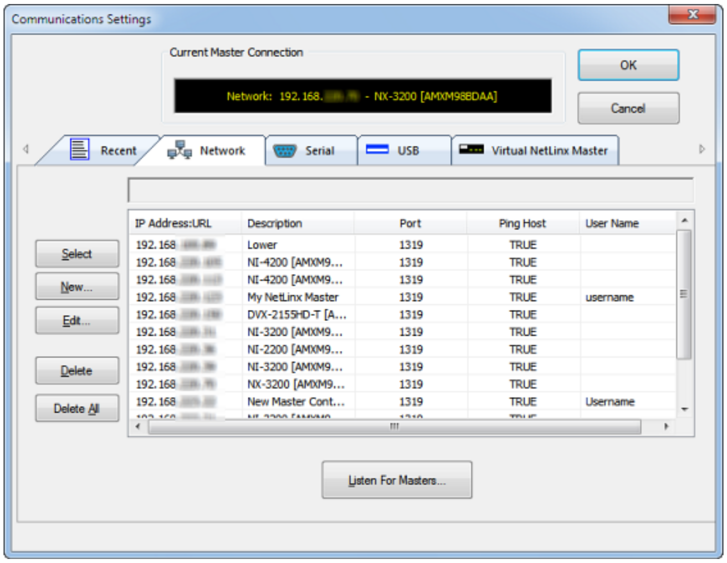
Virtual NetLinx Master: 192.168.[redacted] System: 1

Recent Connections

Type	Description
Network	192.168.[redacted] - NI-4200 [AMXM98BE94]
VNM	192.168.[redacted]
Network	ddswpvbeta -
Network	192.168.[redacted] - DVX-2155HD-T [AMXM96F520]

FIG. 16 NetLinx Studio - Communication Settings dialog (TCP/IP selected)

4. Select the Network tab (FIG. 17).



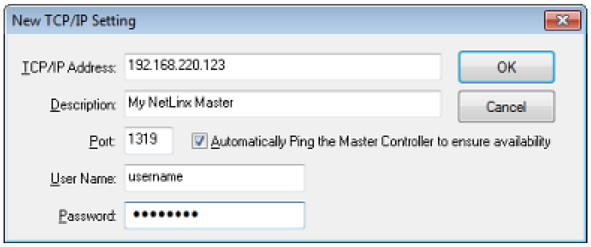
Current Master Connection

Network: 192.168.[redacted] - NX-3200 [AMXM98BDAA]

IP Address:URL	Description	Port	Ping Host	User Name
192.168 [redacted]	Lower	1319	TRUE	
192.168 [redacted]	NI-4200 [AMXM9...	1319	TRUE	
192.168 [redacted]	NI-4200 [AMXM9...	1319	TRUE	
192.168 [redacted]	My NetLinx Master	1319	TRUE	username
192.168 [redacted]	DVX-2155HD-T [A...	1319	TRUE	
192.168 [redacted]	NI-3200 [AMXM9...	1319	TRUE	
192.168 [redacted]	NI-2200 [AMXM9...	1319	TRUE	
192.168 [redacted]	NI-3200 [AMXM9...	1319	TRUE	
192.168 [redacted]	NX-3200 [AMXM9...	1319	TRUE	
192.168 [redacted]	New Master Cont...	1319	TRUE	Username

FIG. 17 Communications Settings dialog - Network tab

5. Click **New** to open the *New TCP/IP Setting* dialog. In this dialog, you can enter both a previously obtained DHCP or static IP address and an associated *Description* for the connection into their respective fields. (FIG. 18):



TCP/IP Address: 192.168.220.123

Description: My NetLinx Master

Port: 1319 ☑ Automatically Ping the Master Controller to ensure availability

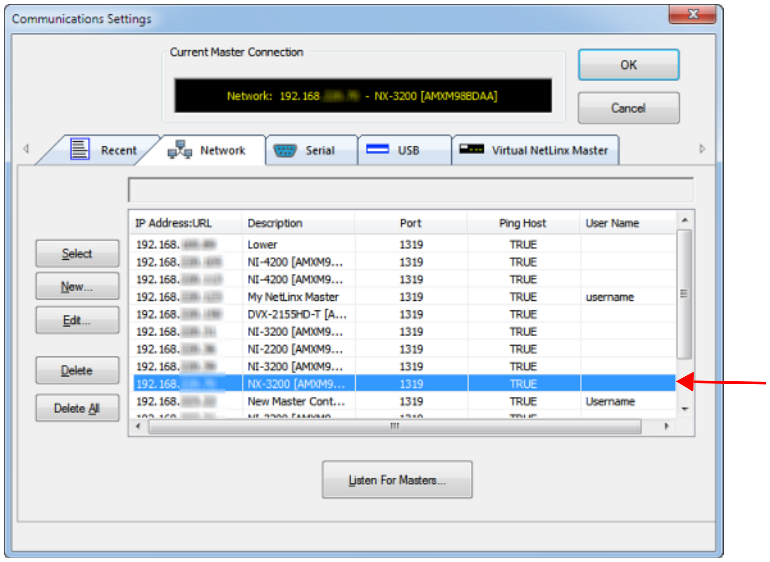
User Name: username

Password: ••••••••

FIG. 18 NetLinx Studio - New TCP/IP Setting dialog

- Verify that the *Automatically Ping the Master Controller to ensure availability* option is selected to make sure the Master is initially responding on-line before establishing full communication.
- If the authentication is required for connecting to the Master at this address, enter a *User Name* and *Password* in the text fields provided.

6. Click **OK** to close the *New TCP/IP Settings* dialog and return to the *Communication Settings* dialog: (FIG. 19).



Current Master Connection

Network: 192.168 [redacted] - NX-3200 [AMXM98BDAA]

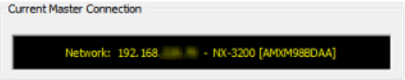
IP Address:URL	Description	Port	Ping Host	User Name
192.168.[redacted]	Lower	1319	TRUE	
192.168.[redacted]	NI-4200 [AMXM9...	1319	TRUE	
192.168.[redacted]	NI-4200 [AMXM9...	1319	TRUE	
192.168.[redacted]	My NetLinx Master	1319	TRUE	username
192.168.[redacted]	DVX-2155HD-T [A...	1319	TRUE	
192.168.[redacted]	NI-3200 [AMXM9...	1319	TRUE	
192.168.[redacted]	NI-2200 [AMXM9...	1319	TRUE	
192.168.[redacted]	NI-3200 [AMXM9...	1319	TRUE	
192.168.[redacted]	NX-3200 [AMXM9...	1319	TRUE	
192.168.[redacted]	New Master Cont...	1319	TRUE	Username

FIG. 19 NetLinx Studio - Communication Settings dialog

a. Click on the new IP address entry in the *List of Addresses* window

b. Click **Select** to use the selected IP address as the current IP address.

7. Click **OK** to save your newly entered information and close the *Communication Settings* dialog and return to the *Communication Settings* dialog. Note the selected IP address is indicated in the *Configuration* field (FIG. 20):



Current Master Connection

Network: 192.168 [redacted] - NX-3200 [AMXM98BDAA]

FIG. 20 NetLinx Studio - Communication Settings dialog (Current Master Connection field indicating the selected IP address)

8. Click **OK** to begin the communication process to your Master (and close the dialog).
   - If you are currently connected to a Master, a pop-up asks whether you would want to stop communication to the current Master and apply the new settings.
   - Click **Yes** to interrupt the current communication from the Master and apply the new settings.

Note: *On the front panel of the NetLinx Master, the STATUS and OUTPUT LEDs should begin to alternately blink during the incorporation. Wait until the STATUS LED is the only LED to blink.*

9. Click the **OnLine Tree** tab in the Workspace window to view the devices on the System. *The default System value is one (1).*

10. Right-click the associated System number and select **Refresh System**. This establishes a new connection to the specified System and populates the list with devices on that system. *The communication method is then highlighted in green on the bottom of the NetLinx Studio window.*

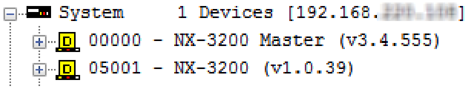
Note: *If the connection fails to establish, a Connection Failed dialog appears. Try selecting a different IP address if communication fails. Press the Retry button to reconnect using the same communication parameters. Press the Change button to alter your communication parameters and repeat the steps above.*

Upgrading Firmware

Overview

The basic process of upgrading firmware on NX-series controllers involves downloading the latest firmware files from *www.amx.com* and using NetLinx Studio to transfer the files to a target NX controller.

Use the OnLine Device tree in NetLinx Studio to view the firmware files currently loaded on the Central Controller. FIG. 21 shows an example OnLine Tree indicating an NX-3200:



```
System     1 Devices [192.168.[redacted]]
  00000 - NX-3200 Master (v3.4.555)
  05001 - NX-3200 (v1.0.39)
```

FIG. 21 NetLinx Studio - Sample OnLine Tree

While the method of upgrading firmware files is the same for all Central Controllers, there are some specific points relative to the specific model and type of controller that must be noted:

NX Controllers - Firmware Files

NX controllers contain two devices (*NX Master* and *Device Controller*), each of which require a separate firmware (*.kit) file.

The NX Master firmware file is not the same as the Device Controller firmware file. These two devices must be kept at compatible firmware versions for proper operation. Therefore, both files should be used when upgrading any firmware associated with the Integrated Controllers.

NX Controllers - Firmware Files	
NX Master Firmware	The on-board **NX Master** is listed first in the OnLine Tree as "**00000 NX Master (<firmware version>)**" For example, the NX Master in FIG. 21 above is "*00000 - NX-3200 Master (v3.4.555)*". • "**00000**" represents ***Device ID 0***, which is reserved for the Master • The number in parenthesis (in this case "*v3.4.555*") is the current NX Master firmware version.
Device Controller Firmware	The **Device Controller** is listed next as "**05001 NX-XXXX (<firmware version>)**" For example, the Device Controller in FIG. 21 above is "*05001 - NX-3200 (v1.0.35)*". • "**05001**" represents ***Device ID 5001***, which is reserved for the Device Control ports. • The number in parenthesis (in this case "*v1.0.35*") is the current Device Controller firmware version.

Before You Start

1. Verify you have the latest version of the NetLinx Studio application installed on your PC.

   NetLinx Studio is available to download from *www.amx.com*. Login to download the latest version. Alternatively, if it is already installed, use the **Web Update** option in NetLinx Studio's Help menu to obtain the latest version.

   The default location for the NetLinx Studio application is **Start** > **Programs** > **AMX Control Disc** > **NetLinx Studio** > **NetLinx Studio**.
2. Verify that a LAN cable is connected from the controller to the LAN Hub.
3. Verify that the controller is powered on.
4. Connect to the controller via IP address.
5. Establish what version of firmware is currently loaded on the controller (see *Verifying the Current Firmware Version* below).

Verifying the Current Firmware Version

Use the OnLine Tree in NetLinx Studio (see FIG. 21 on page 13) to verify which version of each firmware file is currently installed.

Note: *These steps assume that you have already established a connection with the target Central Controller (see the Initial Configuration* section on page 4 *for details).*

1. In NetLinx Studio, click on the **OnLine Tree** tab (in the Workspace Bar) to view the devices on the System.
2. Click **Display** and select **Refresh System** from the context menu. This establishes a new connection to the System and populates the device tree with devices on that system.
3. After the *Communication Verification* dialog indicates active communication between the PC and the Central Controller, verify the Central Controller and associated devices are listed in the OnLine Tree.
4. Check the appropriate product page on *www.amx.com* for the latest *NX Master* and *Device Controller* firmware files for your device.

If necessary, follow the procedures outlined in the following sections to obtain these firmware (*.kit) files from *www.amx.com* and then transfer the new firmware files to the device.

Downloading the Latest Firmware Files from www.amx.com

NetLinx Integrated Controllers

NX-series Controllers require two firmware (*.kit) files: *Master* firmware and *Device* firmware. The Master firmware file is not the same as the Device firmware file.

Both files should be used when upgrading any firmware associated with the Integrated Controllers.

Note: *The process of downloading and transferring firmware files is the same for all types of firmware. However, it is important that the firmware files are upgraded in specific following order for NX-series Controllers (see the Required Order of Firmware Updates* section on page 15*).*

Master and Device Firmware Kit Files for NX-Series Controllers

Below is a table outlining the *Master* and *Device* Firmware (*.kit) files used by NetLinx Integrated Controllers:

Master and Device Firmware Files for NX-Series Controllers	
NX-4200 / 3200 / 2200 / 1200	**Master** Firmware: **SW2106_NX_X200_vx_x_xxx.kit**
	Device Firmware: **SW2106_NX-X200_Device_vx_xx_x.kit**

Downloading NX-Series Controller Firmware Files on www.amx.com

Visit the appropriate product page on www.amx.com for the latest *NX Master* and *Device Controller* firmware (*.kit) files for your NX controller. Firmware file links are available along the right-side of the catalog page (FIG. 22):

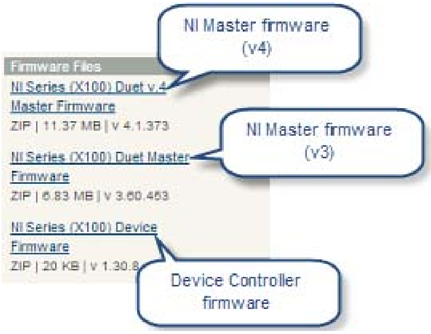

NI Master firmware (v4)
Firmware Files
NI Series (X100) Duet v.4 Master Firmware
ZIP | 11.37 MB | v 4.1.373
NI Master firmware (v3)
NI Series (X100) Duet Master Firmware
ZIP | 6.83 MB | v 3.60.453
NI Series (X100) Device Firmware
ZIP | 20 KB | v 1.30.8
Device Controller firmware

FIG. 22 www.amx.com - sample NI Controller Firmware File links (NI-2100 shown)

Firmware files are bundled in a ZIP file, along with a Readme.TXT file that provides details on this firmware release.

1. Accept the *AMX Licensing Agreement*.
2. Download the ZIP file and unzip the contents to a known location.

Required Order of Firmware Updates

The *Upgrading Firmware via NetLinx Studio* instructions (below) apply equally to all types of firmware files. However, it is important that the firmware files are upgraded in the following order:

1. First, upgrade the **Master** firmware.
2. When that process is complete, upgrade the **Device** firmware.

Upgrading Firmware via USB

All X-Series controllers support firmware upgrades via a USB solid-state drive. You can upgrade via USB by selecting the appropriate .kit file and initiating the upgrade via telnet. The “IMPORT KIT” telnet command causes the controller to search the attached USB drive for all valid .kit files and display the files as a list. From here you can select the .kit file to use and initiate the firmware upgrade. See the *IMPORT KIT* section on page 94 for more information.

Upgrading Firmware via NetLinx Studio

***Note:** These steps assume that you have already established a connection with the target Central Controller (IP connection is preferred.) See the Initial Configuration* section on page 4 *for details.*

1. In NetLinx Studio. click on the **OnLine Tree** tab (in the Workspace Bar) to view the devices on the System.
2. In the OnLine Tree tab, click **Display** and select **Refresh System** from the context menu. Doing so establishes a new connection to the System and populates the device tree with devices on that system.
3. After the *Communication Verification* dialog indicates active communication between the PC and the Central Controller, verify the Master and associated devices (including the *Device Controller*) are listed in the OnLine Tree.
4. In NetLinx Studio, select **Tools** > **Firmware Transfers > Send to NetLinx Device** (FIG. 23):

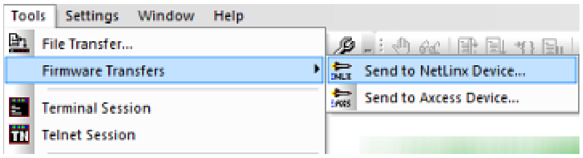
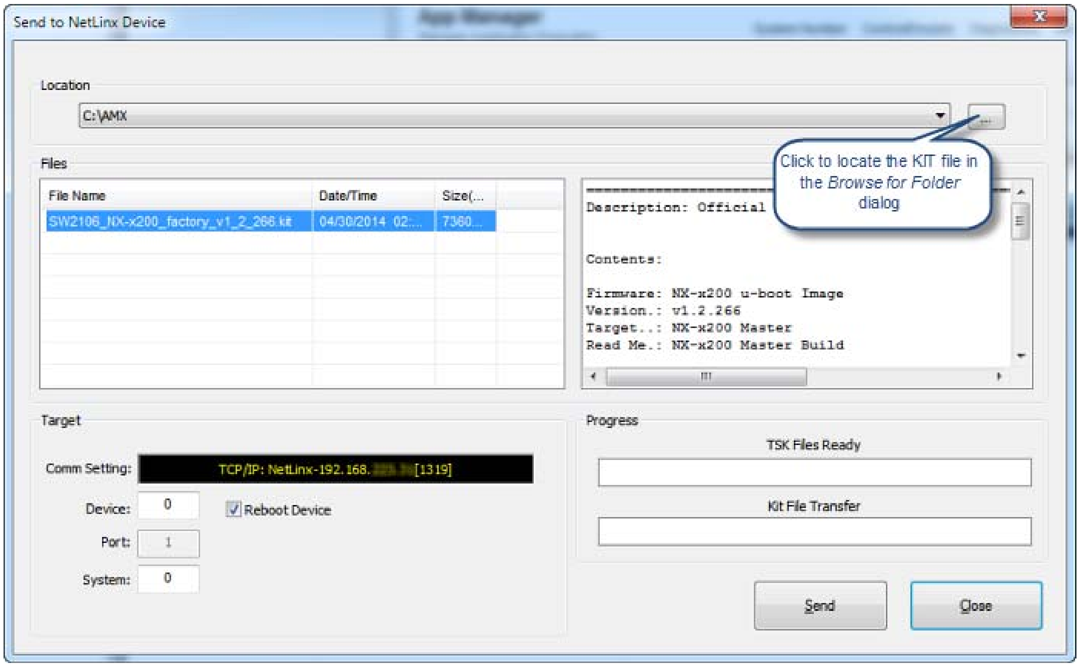


FIG. 23 NetLinx Studio - Tools > Firmware Transfers > Send to NetLinx Device

This opens the *Send to NetLinx Device* dialog.

5. Click the *Browse* button (**...**) to locate and select the firmware (*.kit) file that will be transferred, in the *Browse for Folders* dialog (FIG. 24):



Location: C:\AMX

File Name	Date/Time	Size(...
SW2106_NX-x200_factory_v1_2_266.kit	04/30/2014 02:...	7360...

```
==============================
Description: Official

Contents:

Firmware: NX-x200 u-boot Image
Version.: v1.2.266
Target..: NX-x200 Master
Read Me.: NX-x200 Master Build
```

Comm Setting: TCP/IP: NetLinx-192.168.[redacted][1319]

Device: 0 ☑ Reboot Device

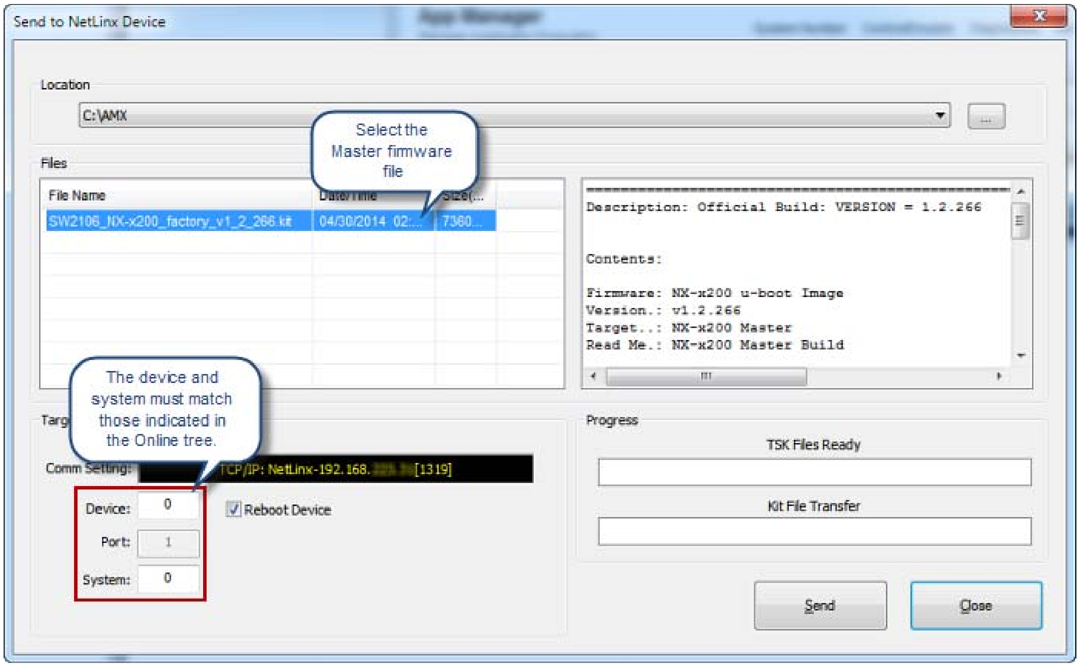
Port: 1

System: 0

FIG. 24 NetLinx Studio - Send to NetLinx Device dialog

The selected file is indicated in the *Files* window.

6. Verify the target's *System* number matches the value listed within the active System folder in the OnLine Tree.
   - The *Device* number is always **0** for the NX Master.
   - Note that the *Port* field is disabled (FIG. 25).



Send to NetLinx Device

Location: C:\AMX

Files

File Name	Date/Time	Size(...
SW2106_NX-x200_factory_v1_2_266.kit	04/30/2014 02:...	7360...

```
====================================================
Description: Official Build: VERSION = 1.2.266


Contents:

Firmware: NX-x200 u-boot Image
Version.: v1.2.266
Target..: NX-x200 Master
Read Me.: NX-x200 Master Build
```

Select the Master firmware file

The device and system must match those indicated in the Online tree.

Comm Setting: TCP/IP: NetLinx-192.168.[redacted][1319]

Device: 0

Port: 1

System: 0

☑ Reboot Device

Progress

TSK Files Ready

Kit File Transfer

FIG. 25 Send to NetLinx Device dialog (showing on-board NX Master firmware update)

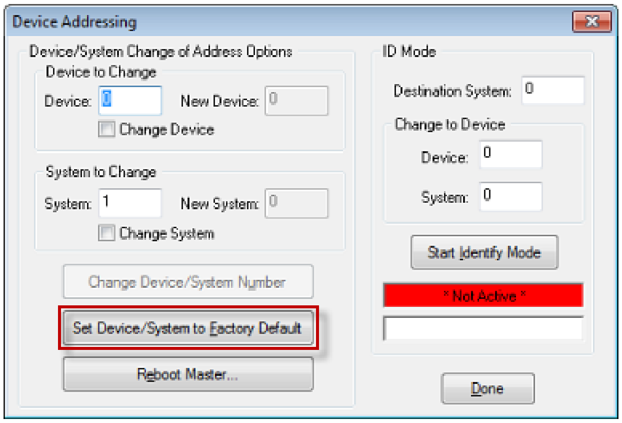
7. Verify that the **Reboot Device** checkbox is selected to reboot the NX controller after the firmware update process is complete (selected by default).
8. Click **Send** to begin the transfer. The file transfer progress is indicated in the *Progress* section of the dialog.
9. Click **Close** once the download process is complete.
10. In the OnLine Tree, right-click on the Master and select **Refresh System**. This establishes a new connection and refreshes the device list and their firmware versions in your system.

Once the process is complete, you can upgrade the remaining firmware files. All device files must be kept at compatible firmware versions for proper operation. Therefore, all files should be used when upgrading any firmware associated with the Integrated Controllers.

Be sure to follow the required order for installing firmware files. See the *Required Order of Firmware Updates* section on page 15 for more information.

Resetting the Factory Default System and Device Values

1. In NetLinx Studio, access the *Device Addressing* dialog:
   - Right-click on any system device listed in the Workspace and select **Device Addressing**.
   - Select **Diagnostics** > **Device Addressing** from the Main menu.
2. Click the **Set Device/System to Factory Default** button (FIG. 26):



Device: 0 New Device: 0
☐ Change Device
System: 1 New System: 0
☐ Change System
Destination System: 0
Device: 0
System: 0

FIG. 26 Device Addressing dialog

This resets both the system value and device addresses (for definable devices) to their factory default settings. The system information (in the **OnLine Tree** tab of the Workspace window) refreshes and then displays the new information.

Note: *By setting the system to its default value (#1), Modero panels that were set to connect to the Master on another System value will not appear in the **OnLine Tree** tab of the Workspace window.*

For example: A Modero touch panel was previously set to System #2. The system is then reset to its default setting of System #1 and then refreshed from within the Workspace window. The panel will not reappear until the system is changed (from within the System Connection page on the Modero) to match the new value and both the Master and panel are rebooted.

3. Click **Done** to close the *Device Addressing* dialog.
4. Click **Reboot** (from the *Tools > Reboot the Master Controller* dialog) and wait for the System Master to reboot.

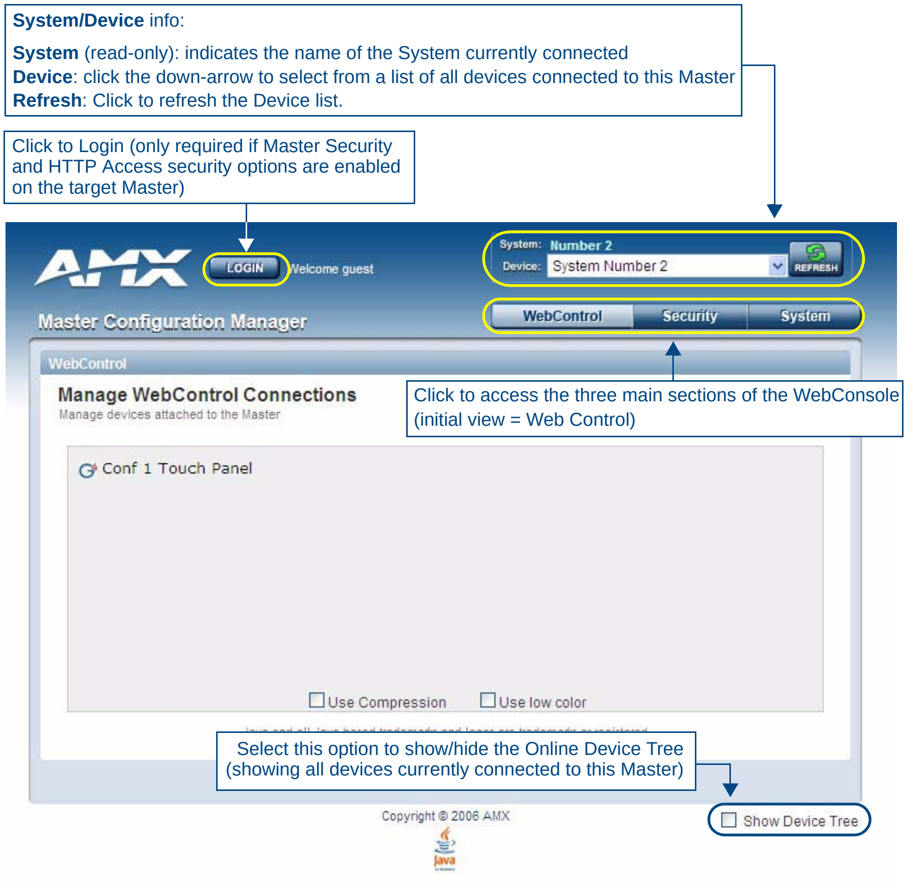
Note: *The STATUS and OUTPUT LEDs should begin to alternately blink during the incorporation. Wait until the STATUS LED is the only LED to blink.*

5. Press **Done** once until the *Master Reboot Status* field reads **Reboot of System Complete**.
6. Click the **OnLine Tree** tab in the Workspace window to view the devices on the System.
7. Right-click the associated System number (*or anywhere within the tab itself*) and select **Refresh System**. This establishes a new connection to the specified System and populates the list with devices on that system.
8. Use **Ctrl+S** to save these changes to your NetLinx Project.

On-Board WebConsole User Interface

WebConsole UI Overview

NetLinx Masters have a built-in WebConsole that allows you to make various configuration settings via a web browser on any PC that has access to the Master. The webconsole consists of a series of web pages that are collectively called the "Master Configuration Manager" (FIG. 27).


System/Device info:

System (read-only): indicates the name of the System currently connected
Device: click the down-arrow to select from a list of all devices connected to this Master
Refresh: Click to refresh the Device list.

Click to Login (only required if Master Security and HTTP Access security options are enabled on the target Master)

Click to access the three main sections of the WebConsole (initial view = Web Control)

Select this option to show/hide the Online Device Tree (showing all devices currently connected to this Master)

FIG. 27 Master Configuration Manager - Web Control Page (initial view)

The webconsole is divided into three primary sections, indicated by three control buttons across the top of the main page (FIG. 28):

FIG. 28 WebConsole Control Buttons

- **Web Control**: This is the option that is pre-selected when the WebConsole is accessed. Use the options in the *Manage Web Control Connections* page to manage G4 Web Control connections (see the *WebConsole - Web Control Options* section on page 33).
- **Security**: Click to access the System Security page. The options in this page allow you to configure various aspects of NetLinx System and Security on the Master (see the *WebConsole - Security Options* section on page 22).
- **System**: Click to access the System Details page. The options on this page allow you to view and configure various aspects of the NetLinx System (see the *WebConsole - System Options* section on page 34).

Accessing the WebConsole

From any PC that has access to the LAN that the target Master resides on:

1. Open a web browser and type the IP Address of the target Master in the Address Bar.
2. Press Enter to access WebConsole for that Master. The initial view is the *Web Control* page (FIG. 27).

Default User Names and Passwords

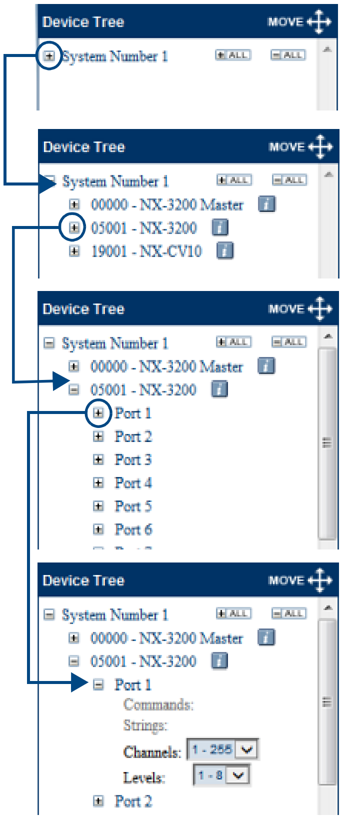
The following table lists the default user names and passwords for accessing the NX-series controllers through NetLinx Studio or the WebConsole.

Default User Names and Passwords		
	User Name	Password
NetLinx Studio	netlinx	password
WebConsole	administrator	password

Device Tree

Click the **Show Device Tree** check box to show/hide the online device tree, which indicates all devices currently connected to this Master. Use the plus and minus symbols to the left of each item in the Device Tree to expand the view to include System devices, ports and individual Port settings.

At the Port view, you can use the Device Tree to make specific port assignments (including Channel and Level assignments) (FIG. 29).



(all collapsed)

(System devices expanded)

(NX-3200 ports expanded)

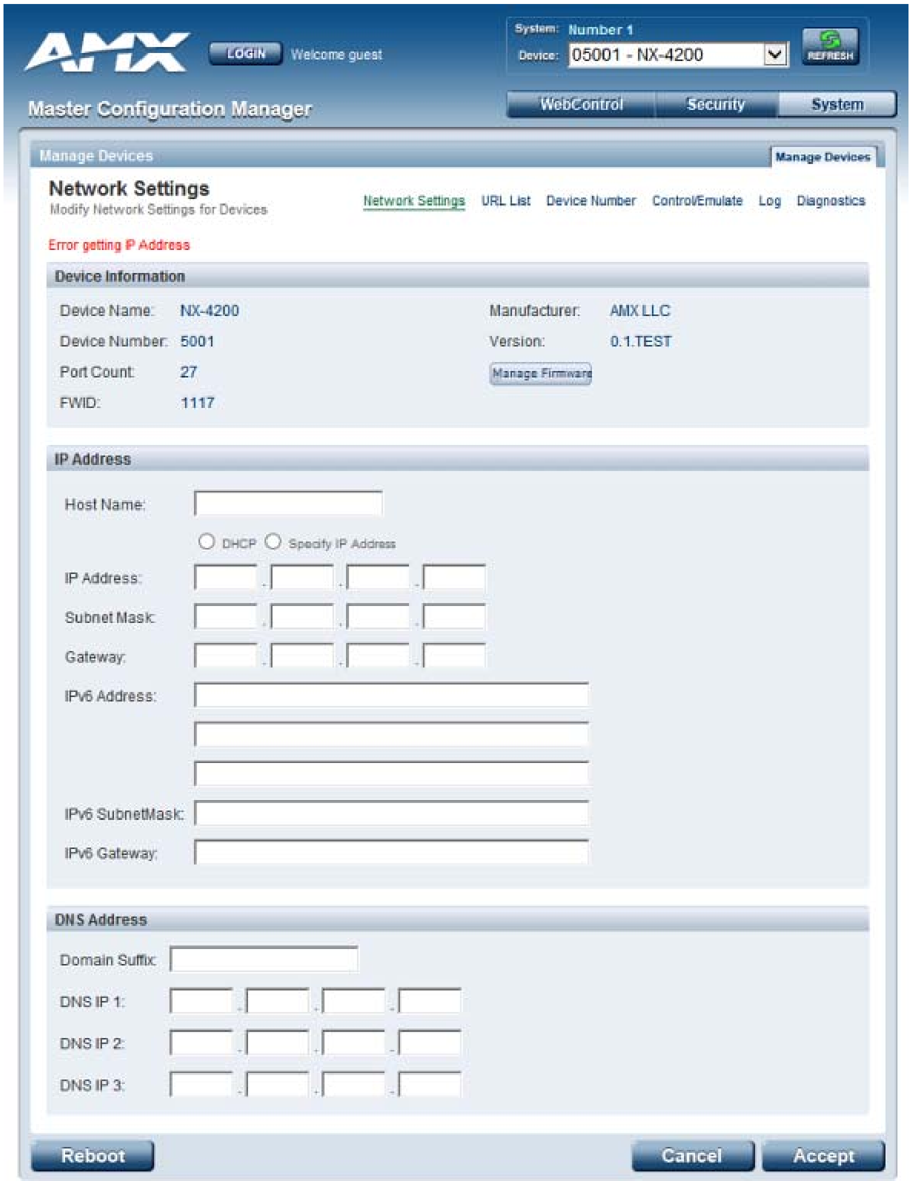
(NX-3200 Port 1 expanded)

FIG. 29 Online Device Tree

Note: *NX-series controllers may list up to 22 ports depending on the model number of the controller. Not all listed port numbers are valid. See the NX-Series Controllers Hardware Reference Guide for a list of valid port numbers for each controller model.*

Device Network Settings Pages

Click on the blue Information (*i*) icon next to any device listed in the Device Tree to access the Network Settings page for the selected device (FIG. 30).



Network Settings

Modify Network Settings for Devices

Error getting IP Address

Device Information

Device Name: NX-4200

Device Number: 5001

Port Count: 27

FWID: 1117

Manufacturer: AMX LLC

Version: 0.1.TEST

IP Address

Host Name:

○ DHCP ○ Specify IP Address

IP Address:

Subnet Mask:

Gateway:

IPv6 Address:

IPv6 SubnetMask:

IPv6 Gateway:

DNS Address

Domain Suffix:

DNS IP 1:

DNS IP 2:

DNS IP 3:

FIG. 30 Example Network Settings page

- Use the options on this page to view/edit the device’s network settings.
- Refer to the *Manage Devices - Network Settings* section on page 67 for details.

ZeroConfig Networking

By default, zeroconf is enabled (*On* option selected). With zeroconf enabled, the Master's web interface will be registered via zeroconf and can be viewed through a zeroconf browser plug-in such as Bonjour for IE.

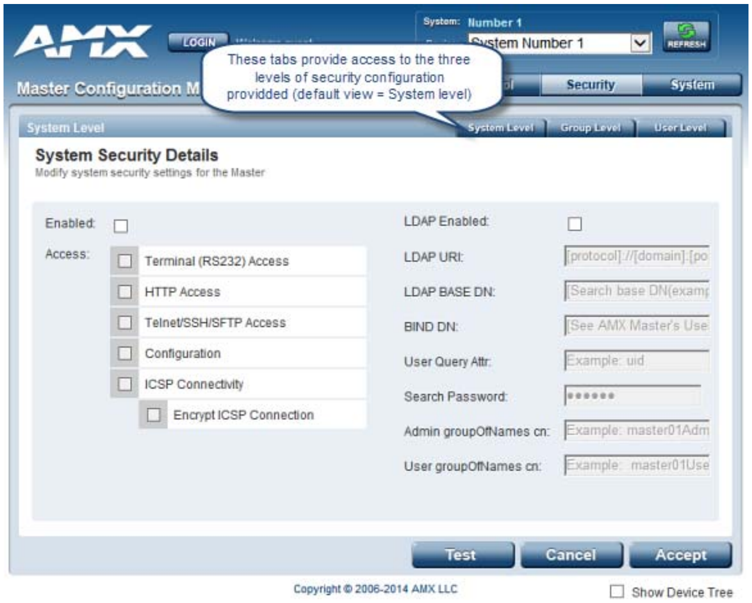
WebConsole - Security Options

Security Overview

The *Security System Details* page is accessed by clicking on the **Security** button. This page allows you to view configure and modify the Master’s security settings at three levels:

- **System Level** - changes made at this level affect the system globally.
  See the *System Security - System Level* section on page 24 for details.
- **Group Level** - changes made at this level affect specific User Groups.
  See the *System Security - Group Level* section on page 27 for details.
- **User Level** - changes made at this level affect individual Users.
  See the *System Security - User Level* section on page 30 for details.

The default view for the option is System Level Security / System Security Settings (FIG. 31).



These tabs provide access to the three levels of security configuration providded (default view = System level)

System Security Details
Modify system security settings for the Master

Enabled: □

Access:
□ Terminal (RS232) Access
□ HTTP Access
□ Telnet/SSH/SFTP Access
□ Configuration
□ ICSP Connectivity
□ Encrypt ICSP Connection

LDAP Enabled: □
LDAP URI: [protocol]://[domain]:[po
LDAP BASE DN: [Search base DN(examp
BIND DN: [See AMX Master's Use
User Query Attr: Example: uid
Search Password: ••••••
Admin groupOfNames cn: Example: master01Adm
User groupOfNames cn: Example: master01Use

□ Show Device Tree

FIG. 31 System Security Details Page (System Security Settings)

***Note:** By default, all System-level security options are disabled.*

Additional security configuration options are available via Terminal/Telnet Commands:

- See the *Accessing the Security Configuration Options* section on page 110.
- Refer to *SET SECURITY PROFILE* on page 101 for information on setting Security Profiles.

Default Security Configuration

By default, the NetLinx Master creates the following accounts, access rights, directory associations, and security options:

Default Security Configuration		
Account 1	Account 2	Group 1
Username: administrator	*Username*: NetLinx	
Password: password	*Password*: password	
Group: administrator	*Group*: none	*Group*: administrator
Rights: All	*Rights*: FTP Access	*Rights*: All
Directory Association: /*	*Directory Association*: none	*Directory Association*: /*
***Note**: The "administrator" user account cannot be deleted or modified with the exception of its password. Only a user with both Configuration access and administrator rights can alter the administrator’s password.*	***Note**: The "NetLinx" user account is compatible with previous NetLinx Master firmware versions. This account is initially created by default and can later be deleted or modified.*	***Note**: The "administrator" group account cannot be deleted or modified.*

- FTP Security is always enabled on the Masters.
- The **Admin Change Password Security** option (in the Group and User Level Security Details pages is enabled by default.
- All other security options are **disabled** by default.

Login Rules

There is no limit to the number of concurrent logins allowed for a single user. This allows for the creation of a single user that is provided to multiple ICSP devices (touch panels, for example) using the same login to obtain access to the Master.

For example, if you have 50 devices connected to a Master, you do not have to create 50 individual user accounts, with one for each device. Instead, you only need to create one which all 50 devices use for access.

The first layer of security for the Master is to prompt a user to enter a valid user name and password before gaining access to a secured feature on the target Master.

Depending on the Security configuration, users may be prompted to enter a valid user name and password before gaining access to various features of the WebConsole. User access is specified by the administrator in the Group and User Level pages of the Security section.

***Note:** This user name and password information is also used by both G5 touch panels (within the System Connection firmware page) and AMX software applications such as NetLinx Studio v 4.0 and above to communicate securely with a Master using encrypted communication.*

User Name and Password Rules

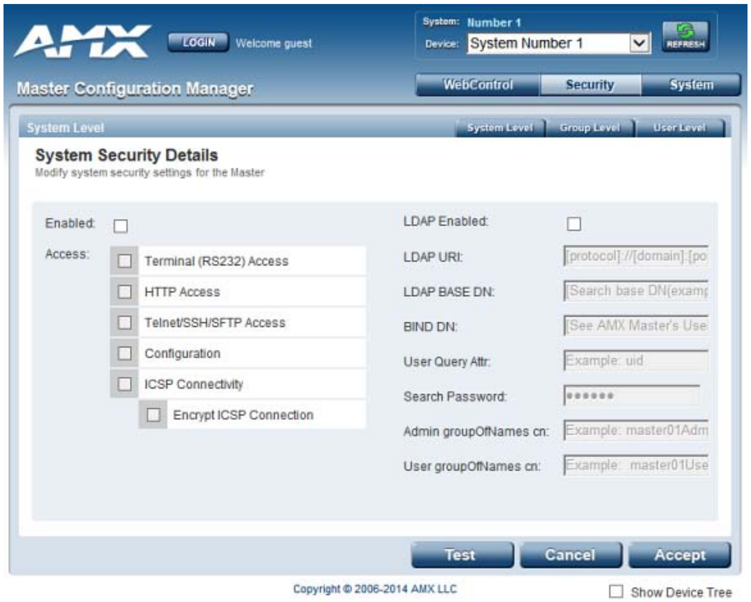
- Case-sensitive
- Must be between 4 and 20 characters
- The following special characters are allowed for use in User Name and Password entries:
  ! ” # $ % & ’ ( ) * + , - . / : ; < = > ? @ [\ ] ^ _ ` { | } ~
  Also allowed are any printable ASCII characters (*including "space"*): A-Z, a-z, 0-9.

System Security - System Level

The *System Level Security* options provide authorized users the ability to alter the current security options of the entire system assigned to the Master.

System Level Security - System Security Settings

Click the **System Security Settings** link to access the System Security Details page (FIG. 32). The options in this page allow you to establish whether the Master will require a valid user name and password be entered prior to gaining access to the configuration options.



System Security Details

Modify system security settings for the Master

Enabled: □

Access:
- □ Terminal (RS232) Access
- □ HTTP Access
- □ Telnet/SSH/SFTP Access
- □ Configuration
- □ ICSP Connectivity
  - □ Encrypt ICSP Connection

LDAP Enabled: □

LDAP URI: [protocol]://[domain]:[po

LDAP BASE DN: [Search base DN(examp

BIND DN: [See AMX Master's Use

User Query Attr: Example: uid

Search Password: ••••••

Admin groupOfNames cn: Example: master01Adm

User groupOfNames cn: Example: master01Use

□ Show Device Tree

FIG. 32 System Security Settings Page

These are global options that enable or disable the login requirement for both users and groups.

Access Options

Check the **Enabled** option on the left side of this page to make the **Access** options available for selection.

The Access options are described in the following table:

Access Options (System Security)	
Option	Description
Enabled:	This option enables the Access options described below. ***Note**: If the Master Security check box is not enabled, all subordinate options are grayed-out and not selectable, meaning that the Master is completely unsecured and can be altered by any user (regardless of their rights).*
Terminal (RS232) Access:	If selected, a valid user name and password is required for Terminal communication via the Master's Program port.
HTTP Access:	If selected, a valid user name and password is required for communication over HTTP or HTTPS Ports, including accessing the WebConsole.
Telnet/SSH/SFTP Access:	If selected, a valid user name and password is required for Telnet Access. Telnet access allows communication over either the Telnet and/or SSH Ports, and Secure FTP access. ***Note**: SSH version 2 (only) is supported.* To establish a secure Telnet connection, an administrator can decide to disable the Telnet Port and then enable the SSH Port. Refer to the *Port Settings* section on page 45 for details.

(System Security) Access Options (Cont.)	
Option	Description
Configuration:	If selected, a valid user name and password is required before allowing a group/user to alter the current Master's security and communication settings via NetLinx Studio. This includes such things as: IP configuration/Reset, URL list settings, Master communication settings, and security parameters.
ICSP Connectivity:	If selected, a valid user name and password is required to communicate with the NetLinx Master via an ICSP connection (TCP/IP, UDP/IP, and RS-232). • This feature allows communication amongst various AMX hardware and software components. This feature works in tandem with the *Require Encryption* option (see below) to require that any application or hardware communicating with the Master must provide a valid user name and password. • In a Master-to-Master system, the Master which accepts the IP connection initiates the authentication process. This configuration provides compatibility with existing implementations and provides more flexibility for the implementation of other devices. ***Note**: The ICSP Connectivity option is required to allow authenticated and/or secure communication between the Master and other AMX hardware/software. To establish an authenticated ICSP connection (where the external AMX hardware/software has to provide a valid user name and password), this option must be enabled.*
Encrypt ICSP Connection:	If selected, this option requires that any data being transmitted or received via an ICSP connection (among the various AMX products) be encrypted, and that any application or hardware communicating with the Master over ICSP must provide a valid user name and password. ***Note**: When enabled, this option requires more processor cycles to maintain.* ICSP uses a proprietary encryption based on RC4 and also requires CHAP-type authentication including user name and password. CHAP (Challenge Handshake Authentication Protocol) authentication is an access control protocol for dialing into a network that provides a moderate degree of security. The CHAP server encrypts the challenge with the password stored in its database for the user and matches its results with the response from the client. If they match, it indicates the client has the correct password, but the password itself never left the client's machine. • When the client logs onto the network, the network access server (NAS) sends the client a random value (the challenge). • The client encrypts the random value with its password, which acts as an encryption key. It then sends the encrypted value to the NAS, which forwards it along with the challenge and user name to the authentication server.

LDAP Options

Check the **LDAP Enabled** option on the right side of this page to make the LDAP options available for selection.

- All parameters are case sensitive and must be entered exactly as they are entered into the LDAP database.
- LDAP Client Configuration can also be done via terminal commands to the NetLinx Master's Program Port - see the *Enabling LDAP via the Program Port* section on page 112 for details.
- See *Appendix A: LDAP Implementation Details* on page 119 for additional information on implementing LDAP on the NetLinx Master.

The LDAP options are described in the following table:

LDAP Options	
Option	Description
LDAP Enabled:	This parameter enables the LDAP configuration parameters described below.
LDAP URI:	This parameter has the syntax **ldap[s]://hostname:port**. • The **ldap:// URL** is used to connect to LDAP servers over unsecured connections. • The **ldaps:// URL** is used to connect to LDAP server over Secure Sockets Layer (SSL) connections. • The **hostname** parameter is the name or IP address, in dotted format, of the LDAP server (for example, *LDAPServer01* or *192.202.185.90*). • The **port** parameter is the port number of the LDAP server (for example, *696*). ***Note:** The standard unsecured port number is **389** and the standard secured port number is **636**.*

LDAP Options (Cont.)	
LDAP BASE DN:	This parameter specifies the Distinguished Name (DN) of an entry in the directory. It identifies the entry that is the starting point of the user search.
BIND DN:	This parameter specifies the Distinguished Name (DN) to use to bind to the LDAP server for the initial search for the user's DN.
User Query Attr.	This LDAP attribute is used for the AMX equipment user search (for example, UID). ***Note:*** *This attribute MUST be unique in the context of the LDAP BASEDN or the search will fail.*
Search Password:	This is the password used for the initial bind to the LDAP server - it is the password associated with BIND DN.
Admin groupOfNames cn:	This parameter is the common name (cn) of the groupOfNames objectClass that contains the member DNs of the AMX equipment users that have administrator privileges.
User groupOfNames cn:	This parameter is the common name (cn) of the groupOfNames objectClass that contains the member DNs of the AMX equipment users that have only user privileges.

- When LDAP is enabled, users are authenticated using the configuration set up on the LDAP server.
- The "*administrator*" user is handled by the local NetLinx Master, and does not connect to the LDAP server for user verification.
- If an administrator password change is desired, LDAP must be disabled, the password changed and saved and then LDAP re-enabled.
- Users may not be added or deleted via the web pages when LDAP is enabled.
- AMX equipment users are set up on the LDAP server with either full access to the master or HTTP access only.
- User access privileges cannot be changed via the web pages.
- As users log onto a NetLinx Master, their user name and access privileges are displayed on the User Security Details page (see *System Security - User Level* section on page 30). This information is stored in the master's RAM but is not written to non-volatile memory, and is lost after a reboot of the Master.
- If a user is removed from the LDAP directory tree, access is denied, and if that user name is on the master's User Security Details web page it is removed.

Configuring ICSP Connectivity with LDAP Enabled

If ICSP connectivity security is desired, the user name and password must be set up on the LDAP server and its DN added as a member to the administrator groupOfNames objectClass. This user name and password must also be present on the master due to the authentication algorithms used for this type security.

Before LDAP is enabled, a user account must be set up with the user name, password and privileges matching the ones stored on the LDAP server.

- If there is a mismatch with the user name or password, the AMX hardware or software component will not be allowed access.
- If there is a mismatch with the access privileges, the master will use the privileges value stored on the server.

Accepting Changes

Click the **Accept** button to save changes on this page. Accepting changes is instantaneous and does not require a reboot.

Testing the Connection to the LDAP Server

After entering and accepting the parameters, the **Test** button (see FIG. 32 on page 24) can be used to test the connection to the LDAP server. This test does a bind to the BIND DN using the Search Password entered.

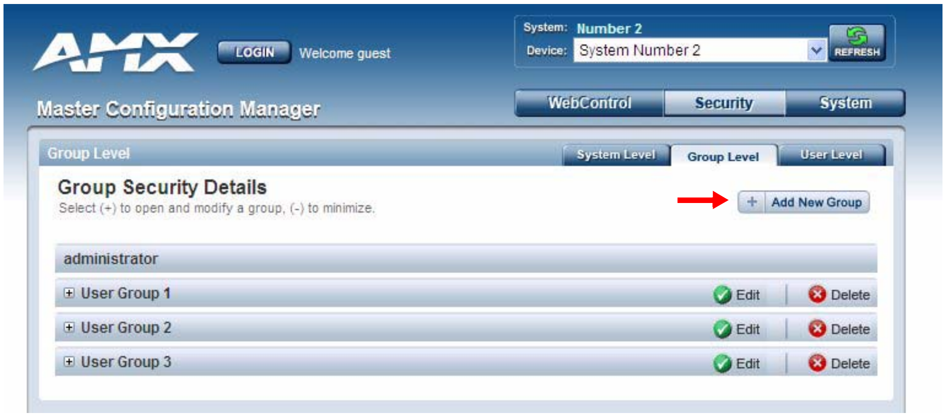
- If the bind is successful, the message *Connection successful* is displayed.
- If the server could not be reached or the bind is unsuccessful, the message *Could not connect to server -- Please check LDAP URI, BIND DN and Search Password settings* is displayed.

Refer to *Appendix A: LDAP Implementation Details* on page 119 for additional information.

System Security - Group Level

Note: *A Group represents a logical collection of individual users. Any properties possessed by a group are inherited by all members of that group.*

Select the *Group Level* tab of the Security Page to access the **Group Security Details** page (FIG. 33).



Group Security Details

Select (+) to open and modify a group, (-) to minimize.

administrator

⊞ User Group 1

⊞ User Group 2

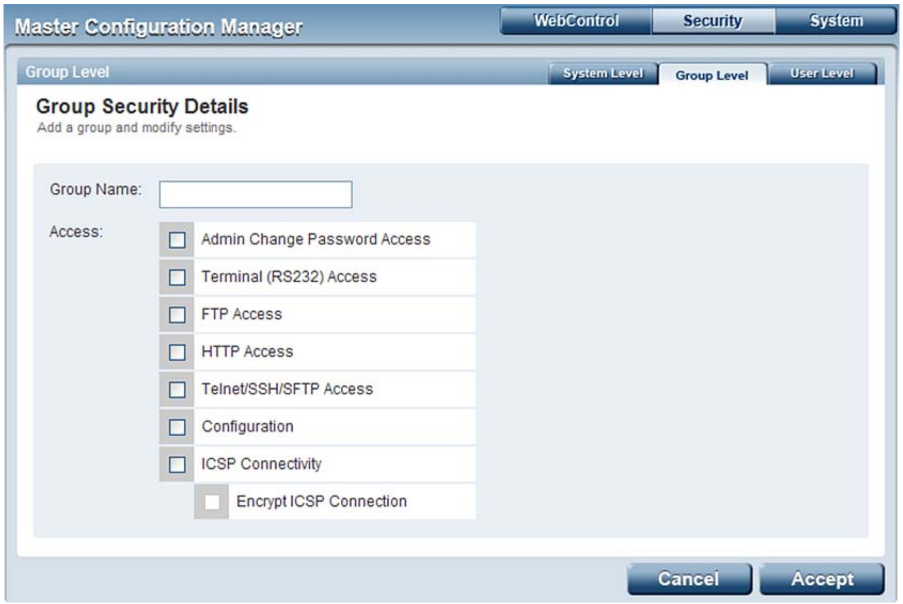
⊞ User Group 3

FIG. 33 Group Security Details page

The options in this page allow authorized users to assign and alter group properties such as creating, modifying, or deleting a group’s rights, and also allows for the definition of the files/directories accessible by a particular group.

Adding a New Group

1. Select the **Group Level** tab (*in the **Security** section*) to open the Group Security Details page.
2. Click the **Add New Group** button (see FIG. 33) to access the **Group Security Details** page (FIG. 34).



Group Security Details

Add a group and modify settings.

Group Name:

Access:

- □ Admin Change Password Access
- □ Terminal (RS232) Access
- □ FTP Access
- □ HTTP Access
- □ Telnet/SSH/SFTP Access
- □ Configuration
- □ ICSP Connectivity
  - □ Encrypt ICSP Connection

FIG. 34 Group Level Security Settings Page (Add a group and modify settings page)

3. In the **Group Name** field, enter a unique name for the new group.
   - The name must be a valid character string consisting of 4 - 20 alpha-numeric characters.
   - The string is case sensitive and must be unique.
   - The word "*administrator"* cannot be used for a new group name since it already exists by default.

4. Enable the security access rights you want to provide to the group. By default, all of these options are disabled. See the *Group and User Security Access Options* section on page 28 for details.
5. Click the **Accept** button to save your changes to the target Master.

   If there are no errors within any of the page parameters, a "*Group added successfully*" displays at the top of the page.

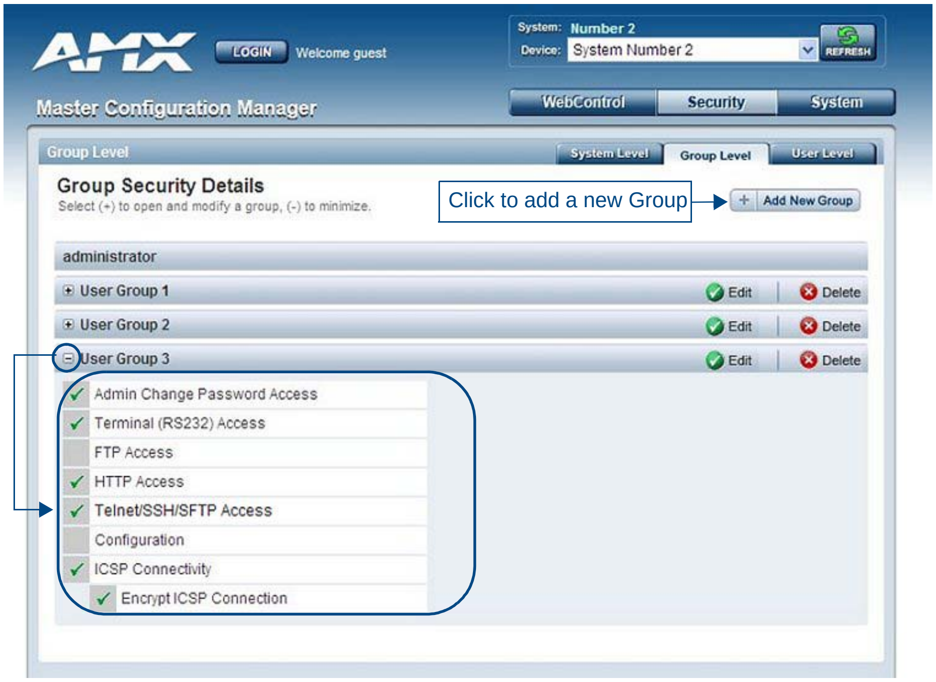
Note: *Security changes made from within the web browser are applied instantly without the need to reboot.*

Group and User Security Access Options

Group and User Security Access Options	
Option	Description
Admin Change Password Access:	This selection enables or disables the Administrator right to change Group and User passwords.
Terminal (RS232) Access:	If selected, a valid user name and password is required for Terminal communication via the Master's Program port.
HTTP Access:	If selected, a valid user name and password is required for communication over HTTP or HTTPS Ports, including accessing the WebConsole.
Telnet/SSH/SFTP Access:	If selected, a valid user name and password is required for Telnet Access. Telnet access allows communication over either the Telnet and/or SSH Ports, and Secure FTP access. ***Note****: SSH version 2 (only) is supported.* To establish a secure Telnet connection, an administrator can decide to disable the Telnet Port and then enable the SSH Port. Refer to the *Manage System - Server Options* section on page 44.
Configuration:	If selected, a valid user name and password is required before allowing a group/user to alter the current Master's security and communication settings via NetLinx Studio. This includes such things as: IP configuration/Reset, URL list settings, Master communication settings, and security parameters.
ICSP Connectivity:	If selected, a valid user name and password is required to communicate with the NetLinx Master via an ICSP connection (TCP/IP, UDP/IP, and RS-232). • This feature allows communication amongst various AMX hardware and software components. This feature works in tandem with the *Require Encryption* option (see below) to require that any application or hardware communicating with the Master must provide a valid user name and password. • In a Master-to-Master system, the Master which accepts the IP connection initiates the authentication process. This configuration provides compatibility with existing implementations and provides more flexibility for the implementation of other devices. ***Note****: The ICSP Connectivity option is required to allow authenticated and/or secure communication between the Master and other AMX hardware/software. To establish an authenticated ICSP connection (where the external AMX hardware/software has to provide a valid user name and password), this option must be enabled.*
Encrypt ICSP Connection:	If selected, this option requires that any data being transmitted or received via an ICSP connection (among the various AMX products) be encrypted, and that any application or hardware communicating with the Master over ICSP must provide a valid user name and password. ***Note****: When enabled, this option requires more processor cycles to maintain.*

Viewing Group Security Settings Details

Click on any Group listed in the *Group Security Details* page to expand the view to show details for the selected user Group (FIG. 35):



Click to add a new Group

Group Security Details

Select (+) to open and modify a group, (-) to minimize.

administrator

⊞ User Group 1

⊞ User Group 2

⊟ User Group 3

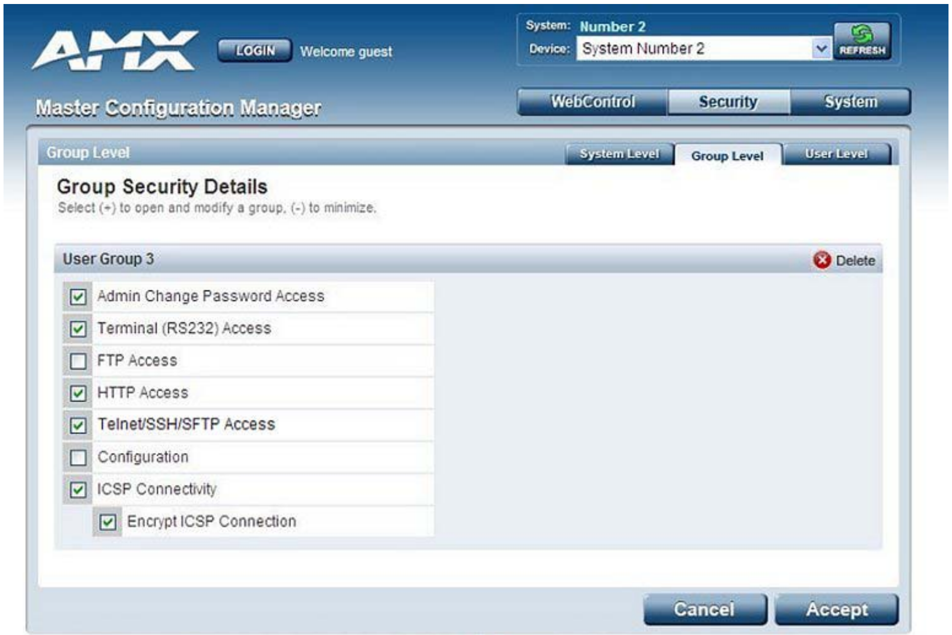
- ✓ Admin Change Password Access
- ✓ Terminal (RS232) Access
- FTP Access
- ✓ HTTP Access
- ✓ Telnet/SSH/SFTP Access
- Configuration
- ✓ ICSP Connectivity
  - ✓ Encrypt ICSP Connection

FIG. 35 Group Security Details Page

- Click the **Edit** button to edit the Security Access options for the selected user group.
- Click **Delete** to delete the selected User Group from the Master.

Modifying the Properties of an Existing Group

1. Select the **Group Level** tab (in the *Security* section) to open the Group Security Details page.
2. Click the **Edit** button to open the *Group Security Details* page for the selected group (FIG. 36).



Group Security Details

Select (+) to open and modify a group, (-) to minimize.

User Group 3

- ☑ Admin Change Password Access
- ☑ Terminal (RS232) Access
- ☐ FTP Access
- ☑ HTTP Access
- ☑ Telnet/SSH/SFTP Access
- ☐ Configuration
- ☑ ICSP Connectivity
  - ☑ Encrypt ICSP Connection

FIG. 36 Group Security Details Page (Edit Group Security Details)

3. Modify the previously configured access rights by enabling / disabling the checkboxes. See the *Group and User Security Access Options* section on page 28 for details.

4. Click the **Accept** button to save your changes to the Master.

   If there are no errors with the modification of any of this page's parameters, a "*Group updated successfully*" is displayed at the top of the page.

Note: *The "administrator" group account cannot be modified or deleted.*

Any properties possessed by groups (ex: access rights, update rights, directory associations, etc.) are inherited by users assigned to that particular group.

Unchecking a security option (which is available within the associated group) does not remove that right from the user. The only way to remove a group's available security right from a target user is either to not associate a group to a user or to alter the security rights of the group being associated.

Deleting a Group

1. Select the **Group Level** tab (in the *Security* section) to open the *Group Security Details* page.

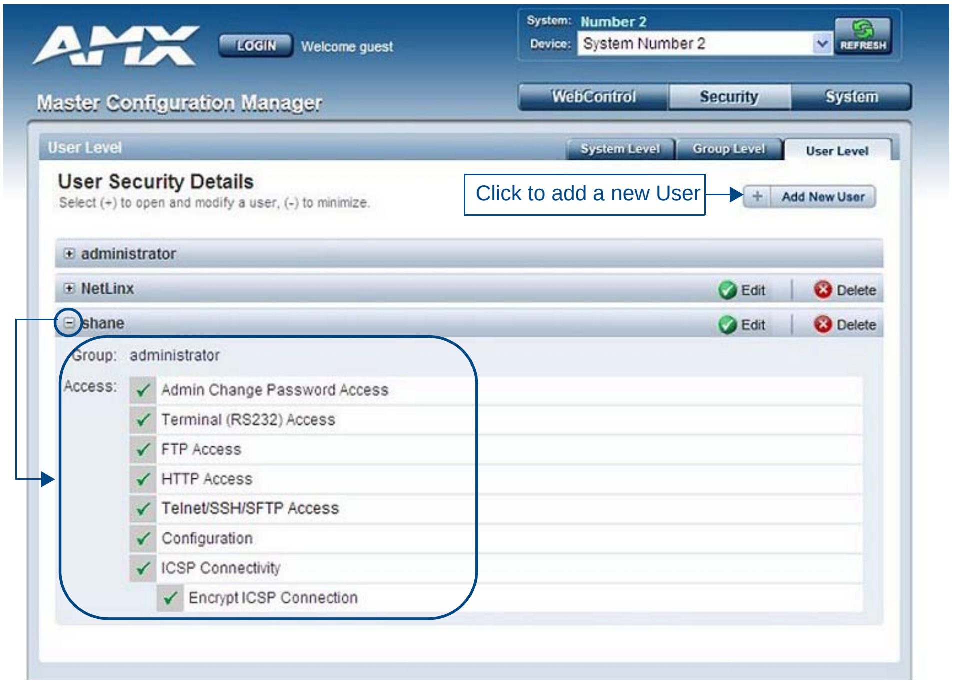
2. Press the **Delete** button to remove the selected group and refresh the page. The system will prompt you to verify this action - click **OK** to proceed.

   - If you are not logged into the Master, you receive a reminder message: *"You must login before Security Settings can be changed"*. In this case, log into the Master and repeat the previous steps.
   - If the group is associated with several users, you might get an error while trying to delete the group. If this happens, change the group association of those specific users utilizing the old group and either give them a new group or assign them (none) as a group. When you return to delete the desired group, you receive a message saying *"Group deleted successfully"*.

3. Click the **Accept** button to save your changes to the Master.

System Security - User Level

Select the *User Level* tab of the Security Page to access the **User Security Details** page (FIG. 37). The options on this page allow authorized users to add/delete User accounts and configure User's Access rights.



User Security Details

Select (+) to open and modify a user, (-) to minimize.

Group: administrator

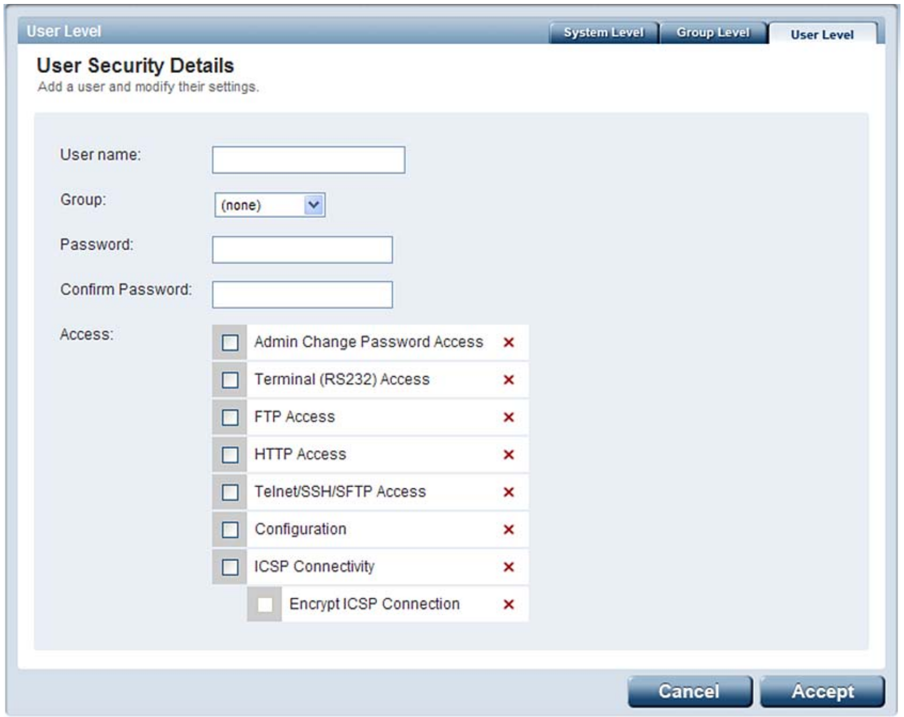
Access:
- ✓ Admin Change Password Access
- ✓ Terminal (RS232) Access
- ✓ FTP Access
- ✓ HTTP Access
- ✓ Telnet/SSH/SFTP Access
- ✓ Configuration
- ✓ ICSP Connectivity
  - ✓ Encrypt ICSP Connection

FIG. 37 User Security Settings Page

Note: *A **User** represents a single client of the Master, while a **Group** represents a collection of Users. Any properties possessed by a Group are inherited by all of the Users in the group.*

Adding a New User

1. Select the **User Level** tab (in the *Security* section) to open the User Security Details page.
2. Click the **Add New User** button (see FIG. 37) to access the Add/Modify User page (FIG. 38).



User Security Details

Add a user and modify their settings.

User name:	
Group:	(none)
Password:	
Confirm Password:	
Access:	□ Admin Change Password Access ✕ □ Terminal (RS232) Access ✕ □ FTP Access ✕ □ HTTP Access ✕ □ Telnet/SSH/SFTP Access ✕ □ Configuration ✕ □ ICSP Connectivity ✕ □ Encrypt ICSP Connection ✕

FIG. 38 User Security Settings Page (Add/Modify User page)

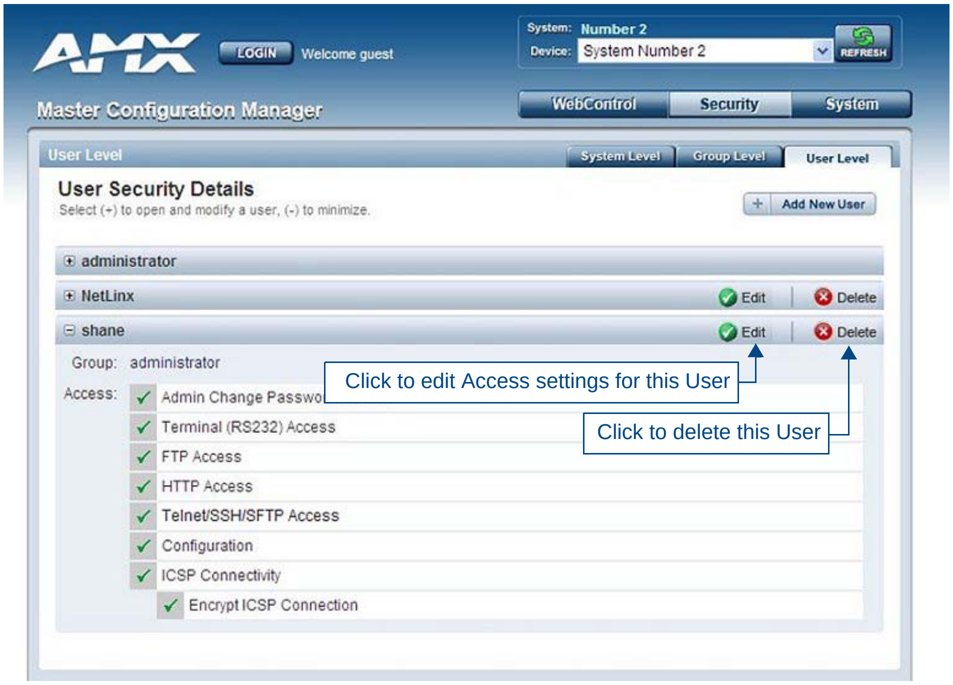
3. In the **User Name** field, enter a unique name for the new group.
   - The name must be a unique alpha-numeric character string (4 - 20 characters), and is case sensitive.
   - The words "*administrator" and "NetLinx"* cannot be used since they already exist by default.
4. In the **Group** options menu, choose from a list of groups and associate the rights of the group to the new user.
5. Enter a user password in both the **Password** and **Password Confirm** fields.

   The password must be a unique alpha-numeric character string (4 - 20 characters), and is case sensitive.
6. Enable the security access rights you want to provide to the user. See the *Group and User Security Access Options* section on page 28 for details.
7. Click the **Accept** button to save your changes to the Master.

Note: *Any security changes made to the Master from within the web browser are instantly reflected within a Terminal session without the need to reboot.*

Viewing and Editing User Security Settings

Click on any User listed in the *User Security Details* page to view and edit security settings for the selected User (FIG. 39):



System: Number 2
Device: System Number 2

User Security Details
Select (+) to open and modify a user, (-) to minimize.

⊞ administrator
⊞ NetLinx
⊟ shane

Group: administrator

Access:
- ✓ Admin Change Passwo
- ✓ Terminal (RS232) Access
- ✓ FTP Access
- ✓ HTTP Access
- ✓ Telnet/SSH/SFTP Access
- ✓ Configuration
- ✓ ICSP Connectivity
  - ✓ Encrypt ICSP Connection

Click to edit Access settings for this User

Click to delete this User

FIG. 39 User Level Security Settings Page (Viewing User Security Settings Details)

- Click the **Edit** button to edit the Security Access options for the selected User.
- Click **Delete** to delete the selected User from the Master.

Deleting a User

1. Select the **User Level** tab (in the *Security* section) to open the User Security Details page.
2. Press the **Delete** button to remove the selected User and refresh the page. The system will prompt you to verify this action - click **OK** to proceed.

   If you are not logged into the Master, you receive a reminder message: *"You must login before Security Settings can be changed"*. In this case, log into the Master and repeat the previous steps.
3. Reboot the Master via the **Reboot** button on the Manage System Page (select the **System** control button to access).

Wired 802.1X support

The X-Series controllers support 802.1X, an IEEE Standard for Port-based Network Access Control. The X-Series controller will act as a supplicant (client device) to an 802.1X enabled network and will present customer provided X.509 certificates to be allowed access to protected networks.

To enable 802.1X, you must load an 802.1X certificate file to your controller using NetLinx Studio. Once you add the certificate file to your workspace, NetLinx Studio transfers the file to the appropriate directory on the controller.

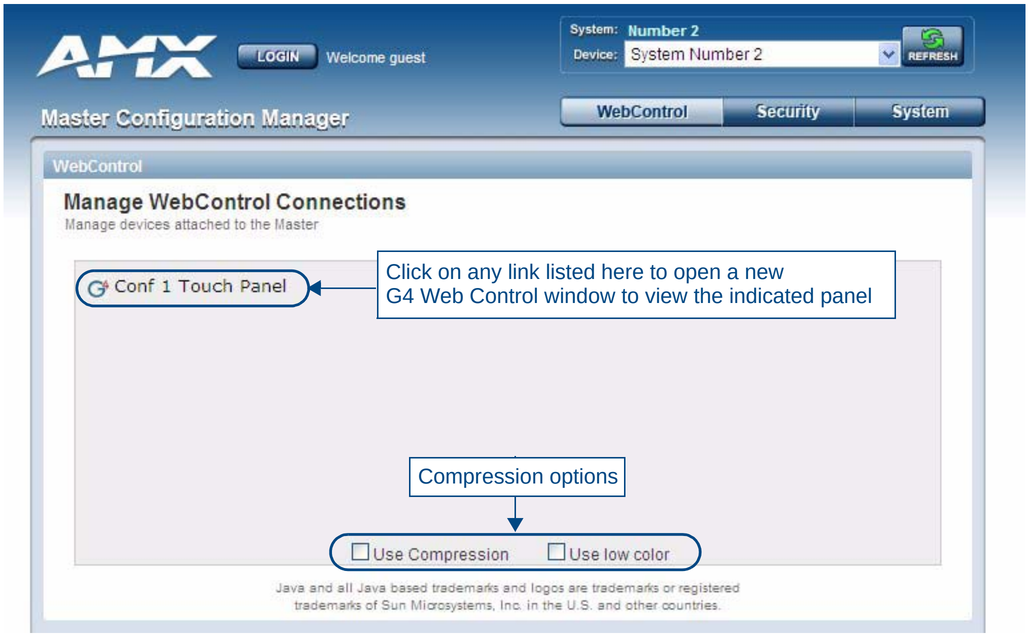
1. Click to select (highlight) a System (in the Workspace tab of the Workspace Bar).
2. Right-click on the **Other** folder to access the Other File Folder context menu, and select **Add Existing Other File**.
3. In the Add Existing Other File dialog, locate and select the certificate file (.crt) that you want to add to the selected System. Change the Files of Type option to All Files (*.*) to look for other file types, if necessary.
4. Click **Open** to access the File Properties dialog, where you can view/edit general file information for the selected file.
5. Click **OK** to add the file to the selected System. The file should now appear in the Other folder under the selected System.

WebConsole - Web Control Options

Manage Web Control Connections

The Web Control page is accessed by clicking on the **Web Control** button (FIG. 40). This page allows you to view all touch panels running the G4 Web Control application.

Each G4 Web Control-equipped touch panel connected to this Master is indicated by a link. Click on any of the links to open a new G4 Web Control window, displaying the selected panel, using the native resolution of the target panel. For example, a CA15 panel link opens a new G4 Web Control window at 800 x 600 resolution.



LOGIN
Welcome guest
System: Number 2
Device: System Number 2
REFRESH
Master Configuration Manager
WebControl
Security
System
WebControl
Manage WebControl Connections
Manage devices attached to the Master
Conf 1 Touch Panel
Click on any link listed here to open a new G4 Web Control window to view the indicated panel
Compression options
□ Use Compression
□ Use low color
Java and all Java based trademarks and logos are trademarks or registered trademarks of Sun Microsystems, Inc. in the U.S. and other countries.

FIG. 40 Manage Web Control Connections page (populated with 1 compatible G4 touch panel)

To establish a secure connection between the touch panel and the target Master, the panel must be using a valid user name and password (*that can be matched to a previously configured user on the target Master*) and the **ICSP Connectivity** option must be enabled within the System Level Security page.

Compression Options

The checkboxes at the bottom of this page allow you to choose from two compression options. Use compression to decrease response delay when viewing G4 Web Control windows over a bandwidth-restricted network, or over the Internet. By default, both compression options are disabled.

- **Use Compression** allows you to specify that the transmitted data packets be compressed. This speeds up the visual responses from the panel by minimizing the size of the information relayed through the web and onto the screen.
- **Use Low Color** allows you to specify the number of colors used to display the image from the panel be reduced. By reducing the numbers of colors, the size of the information is reduced and the response delay is decreased.

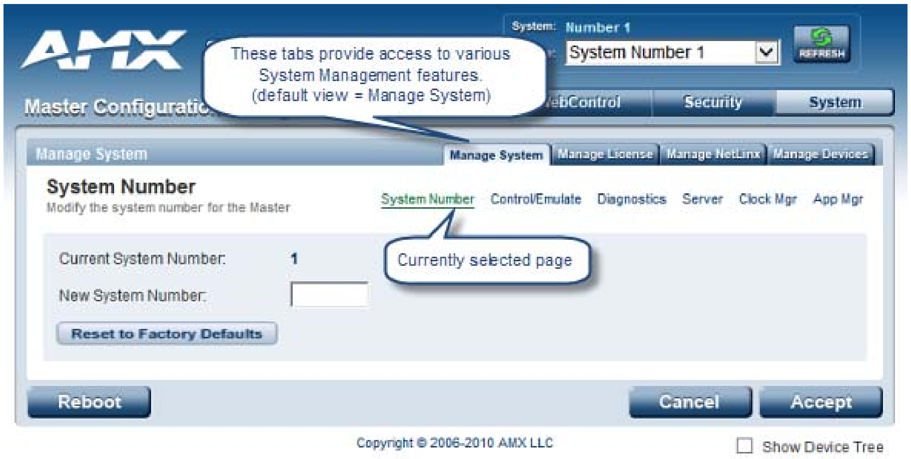
WebConsole - System Options

System Overview

The *Manage System* page is accessed by clicking on the **System** button. This page allows you to view and configure various aspects of the NetLinx System, separated by four tabs:

- **Manage System** - Options in this tab allow you to view/change the Master's *System Number*, Control/ Emulate system devices, perform Diagnostics, configure Server settings and set the time/date via the Clock Manager. See the *System - Manage System* section on page 34 for details.
- **Manage License** - Options in this tab allow you to add device licenses (Product ID and License Key) to the Master. See the *System - Manage License* section on page 54 for details.
- **Manage NetLinx** - Options in this tab allow you to view a detailed list of NetLinx devices connected to the Master. See the *System - Manage NetLinx* section on page 56 for details.
- **Manage Devices** - Options in this tab allow you to view the details of additional attached devices (including module-supported third-party devices). See the *System - Manage Devices* section on page 57 for details.

The default view for the System option is Manage System / System Number (FIG. 41).



These tabs provide access to various System Management features. (default view = Manage System)

System Number

Modify the system number for the Master

Current System Number: 1

New System Number:

Currently selected page

FIG. 41 Manage System tab (System Number)

System - Manage System

The **Manage System** tab contains links to several different System-related configuration pages, as described in the following subsections:

Manage System - System Number

The options on this page display the current System Number assigned to the target Master (read-only), and allow you to change the system number (see FIG. 41).

Changing the System Number on the Master

1. Enter the new numeric value into the **New System Number** field.
2. Click the **Accept** button to save this new value to the system on the target Master. The message "*System number changed to X. Master must be rebooted for the change to take effect.*", reminds you that the Master must be rebooted before the new settings take effect.
3. Click **Reboot** to reboot the target Master. The Device Tree then reads "*Rebooting...*". After a few seconds, the Device Tree refreshes with the current system information (including the updated system number assignment). If the Device Tree does not refresh within a few minutes, press the **Refresh** button and reconnect to the Master.

Using Multiple NetLinx Masters

When using more than one Master, each unit must be assigned to a separate System value. A Master’s System value can be changed but **it’s device Address must always be set to zero (00000)**. The Device Addressing dialog will not allow you to alter the NetLinx Master address value.

Example: Using an NX-2200 and NX-4200:

- The NI-2200 could be assigned to **System 1** (with an Address of 00000).
- The NI-4200 could be assigned to **System 2** (with an Address of 00000).

Resetting the Master Controller to the Factory Defaults Configuration

Click the **Reset To Factory Defaults** button. This resets the Master to its’ factory default state. This includes:

- Removal of all security settings
- Removal of all user files
- Resetting to DHCP
- Loading an empty NetLinx program.

Once reset, the Master will be effectively in an out-of-box state.

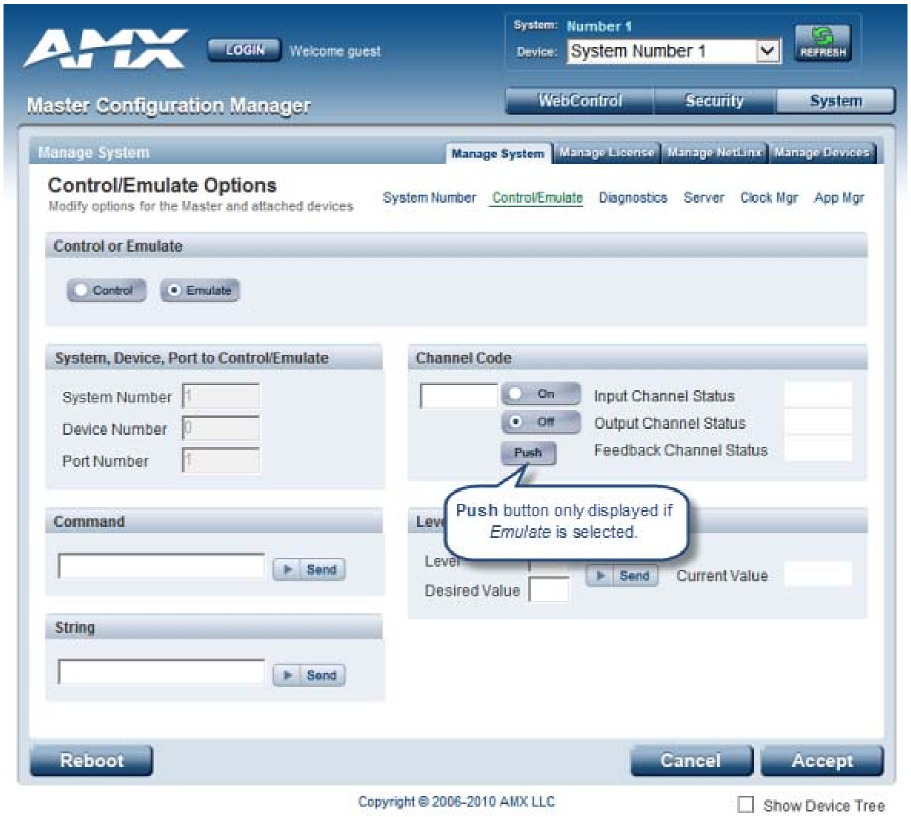
Note: *It may be necessary to refresh the browser window after the master has finished booting (click **Refresh**).*

Manage System - Control/Emulate Options

Click the **Control/Emulate** link (in the *Manage System* tab) to access the Control/Emulate Options page (FIG. 42). The options on this page allow you to *Control* or *Emulate* a device connected to this Master.

Device Control/Emulation is accomplished by manipulating a target device's channels, levels, and sending both send commands and strings to the device.

- To *Control* a device means that the program generates messages which appear to a specified device to have come from the Master.
- To *Emulate* a device means that the program generates messages which appear to the Master to have come from a specified device (physical or virtual). When *Emulate* is selected, a **Push** button is added to the Channel Code section (see FIG. 42).



System: Number 1

Device: System Number 1

○ Control ● Emulate

System Number: 1

Device Number: 0

Port Number: 1

○ On ● Off

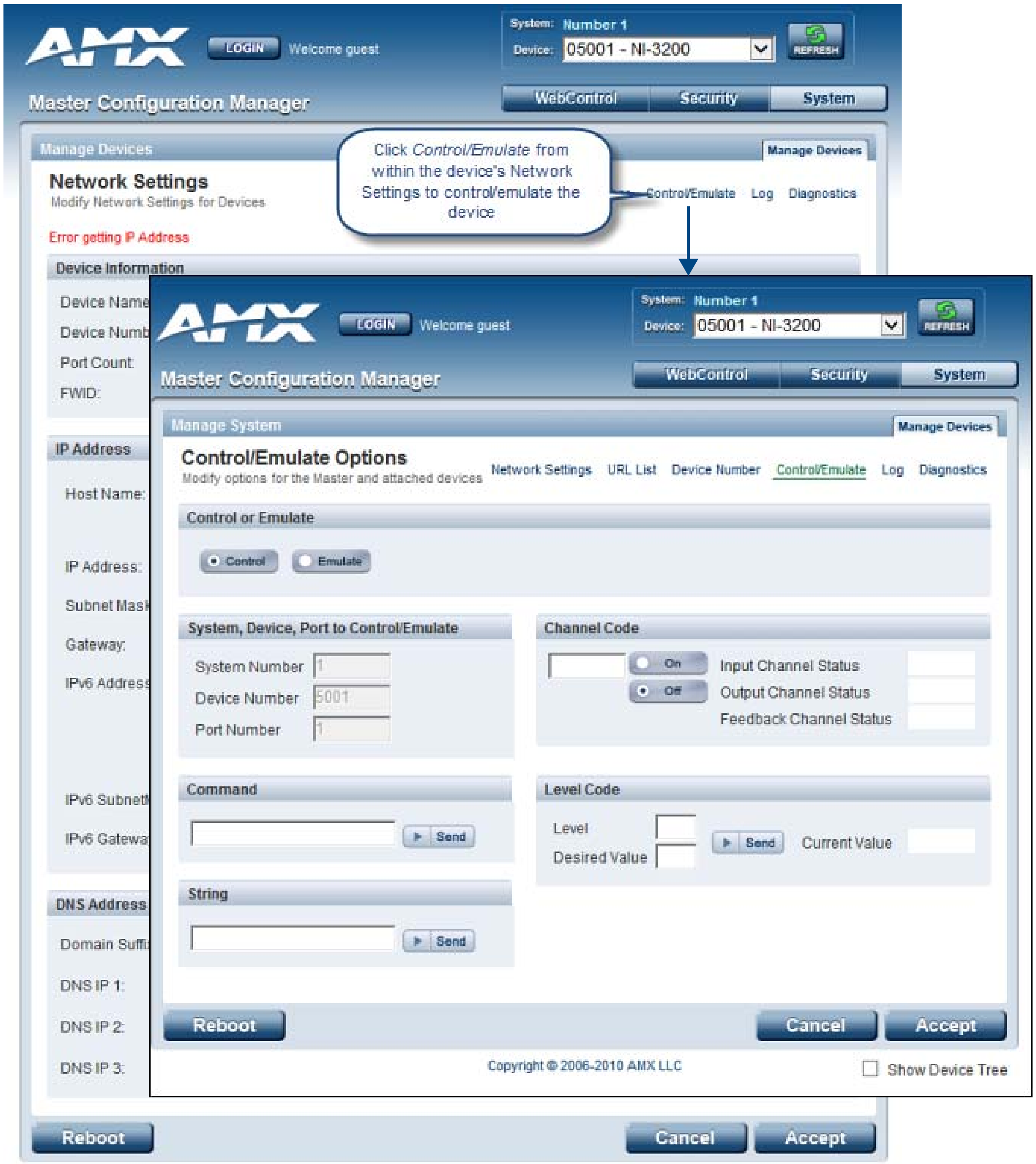
Push button only displayed if *Emulate* is selected.

FIG. 42 Manage System tab (Control/Emulate)

***Note:** The System Number, Device Number, and Port Number fields are read-only. Instead of specifying these values for a System Device, select a device via the Device Tree to populate these fields with that device's information.*

Controlling or Emulating a System Device

1. Select the device that you want to Control or Emulate, via the Device Tree:
   a. Click the **Show Device Tree** option to show the Device Tree window (if it is not already enabled).
   b. In the Device Tree, click on the *Information* (***i***) icon for the device that you want to control or emulate. This opens a Network Settings page showing network configuration details for the selected device. See the *Device Network Settings Pages* section on page 21 for details.
   c. Click on the *Control/Emulate* link. This opens a Control/Emulate Options page for the selected device (FIG. 43).


Click *Control/Emulate* from within the device's Network Settings to control/emulate the device

System: Number 1
Device: 05001 - NI-3200

System Number 1
Device Number 5001
Port Number 1

FIG. 43 Select Control/Emulate from within a selected Device's Network Settings page

2. Select either the **Control** or **Emulate** option.

3. In the *Channel Code* section, enter a valid Channel number to emulate Channel messages (i.e., Push/Release, CHON, and CHOFF) for the specified <D:P:S>.
   - The Channel number range is **1 - 65535**.
   - Select the **On** or **Off** buttons to Emulate Channel ON (CHON) and Channel OFF (CHOFF) messages for the specified <D:P:S>.

4. Select the **Push** button to Emulate a push/release on the specified channel (not displayed if the *Control* option is selected). Click and hold the **Push** button to observe how the device/Master responds to the push message.
5. In the *Level Code* section, enter a valid Level number and Level data value for the specified <D:P:S> and press the **Send** button to transmit the level data.
   - The *Level number* range is **1 - 65535**.
   - The table below lists the valid Level data types and their ranges:

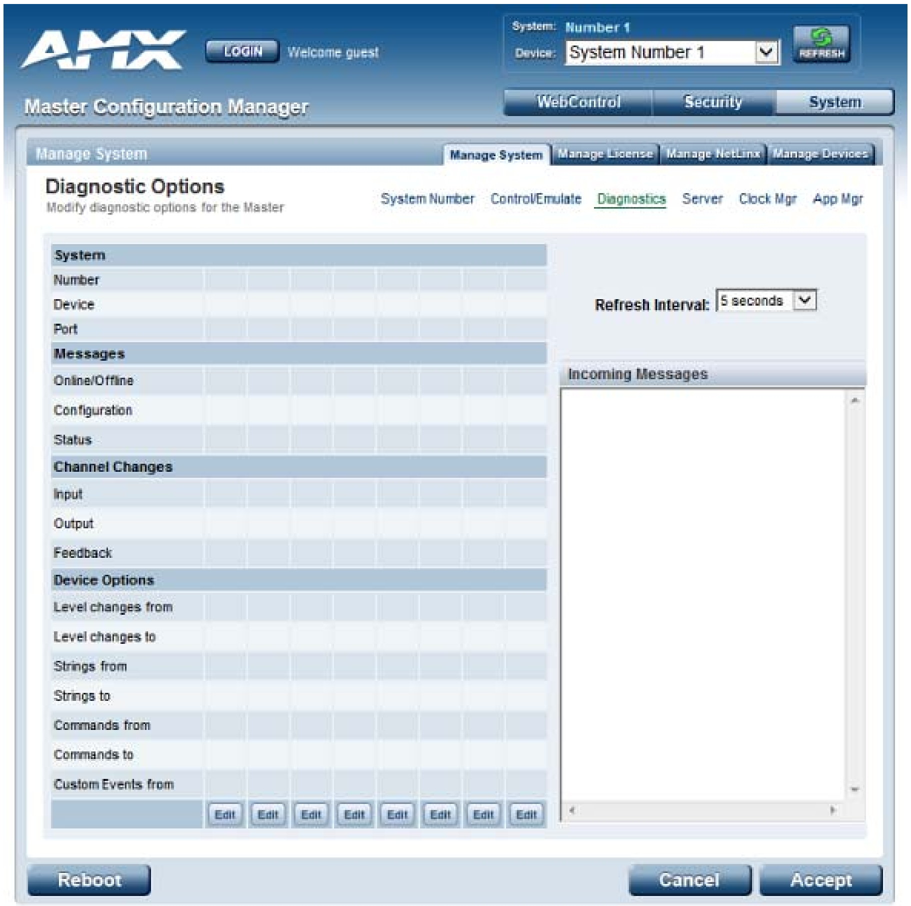
Level Data Type	Minimum Value	Maximum Value
CHAR	0	255
INTEGER	0	65535
SINTEGER	-32768	32767
LONG	0	429497295
SLONG	-2147483648	2147483647
FLOAT	-3.402823466e+38	3.402823466e+38

6. In the *Command* and *String* fields, enter any character strings that can be sent as either a String or Command, and press **Send** to transmit to the Master.
   - When entering a **Send Command**, do not include the "send c" or "SEND_COMMAND" in the statement - only type what would normally occur within the quotes (but don't include the quotes either).

     For example to send the "CALIBRATE" send command, type **CALIBRATE** (no quotes) rather than SEND_COMMAND <dev> "CALIBRATE".
   - **String Expressions** start and end with double quotes (**" "**). Double quotes are not escaped, rather they are embedded within single quotes. String expressions may contain string literals, decimal numbers, ASCII characters and hexadecimal numbers (pre-pended with a **$**), and are comma-delimited.
   - **String Literals** start and end with single quotes (**'**). To escape a single quote, use three single quotes (**'''**).

Manage System - Diagnostics Options

Click the **Diagnostics** link (in the *Manage System* tab) to access the Diagnostics Options page (FIG. 44). The options on this page allow authorized users to enable and monitor various diagnostic messages coming from and going to System Devices.



System: Number 1

Device: System Number 1

Diagnostic Options

Modify diagnostic options for the Master

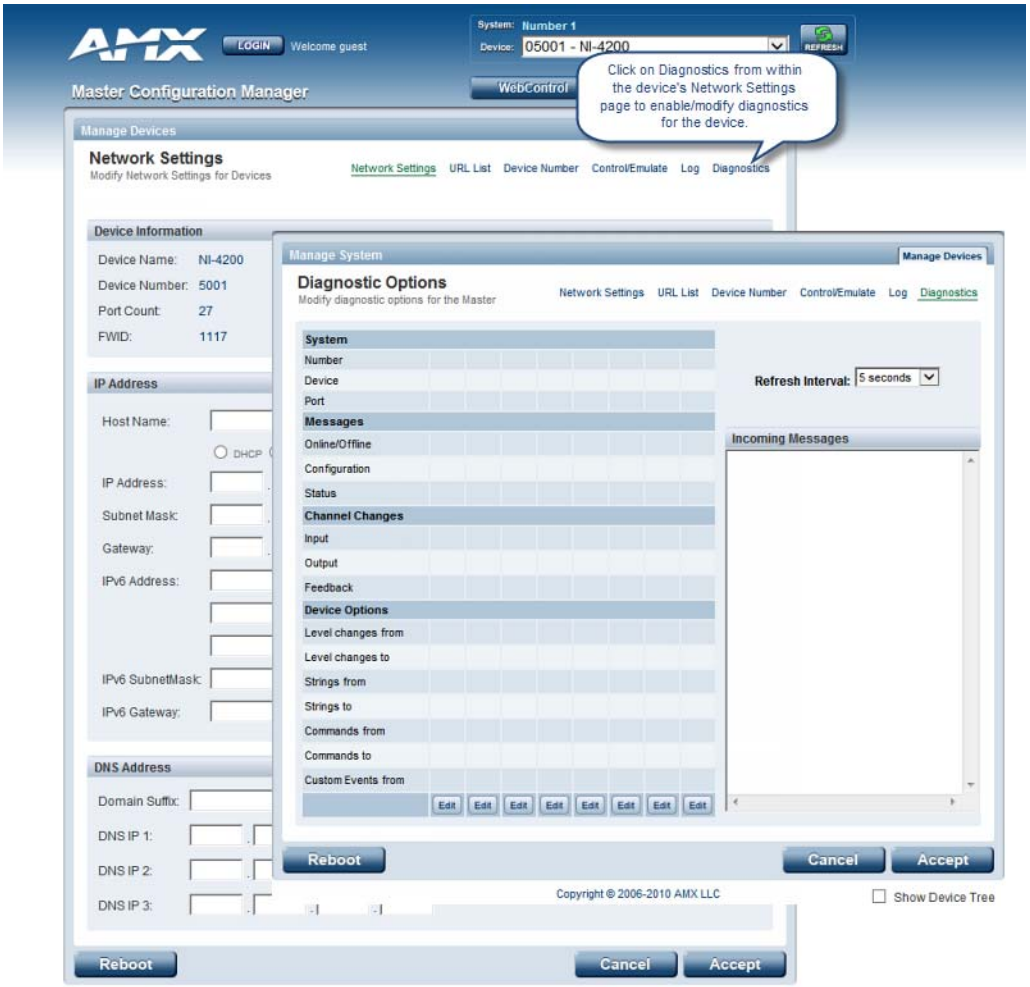
Refresh Interval: 5 seconds

FIG. 44 Diagnostics Options page

Note: *The System Number, Device Number, and Port Number value fields are read-only (disabled). Instead of specifying these values for a System Device, select a device via the Device Tree to populate these fields with that device's values, as described below.*

Enabling Diagnostics on a Selected System Device

1. Select the device that you want to Control or Emulate via the Device Tree:
   a. Click the **Show Device Tree** option to show the Device Tree window (if it is not already enabled).
   b. In the Device Tree, click on the Information (***i***) icon for the device for which you want to enable or modify Diagnostics options. This opens a Network Settings page showing detailed information on the selected device (including network configuration details). An example Network Settings page is shown in FIG. 45:
   c. Click on the **Diagnostics** link. This opens a Diagnostics Options page for the selected device (FIG. 45).



Click on Diagnostics from within the device's Network Settings page to enable/modify diagnostics for the device.

System: Number 1

Device: 05001 - NI-4200

Device Name: NI-4200

Device Number: 5001

Port Count: 27

FWID: 1117

Refresh Interval: 5 seconds

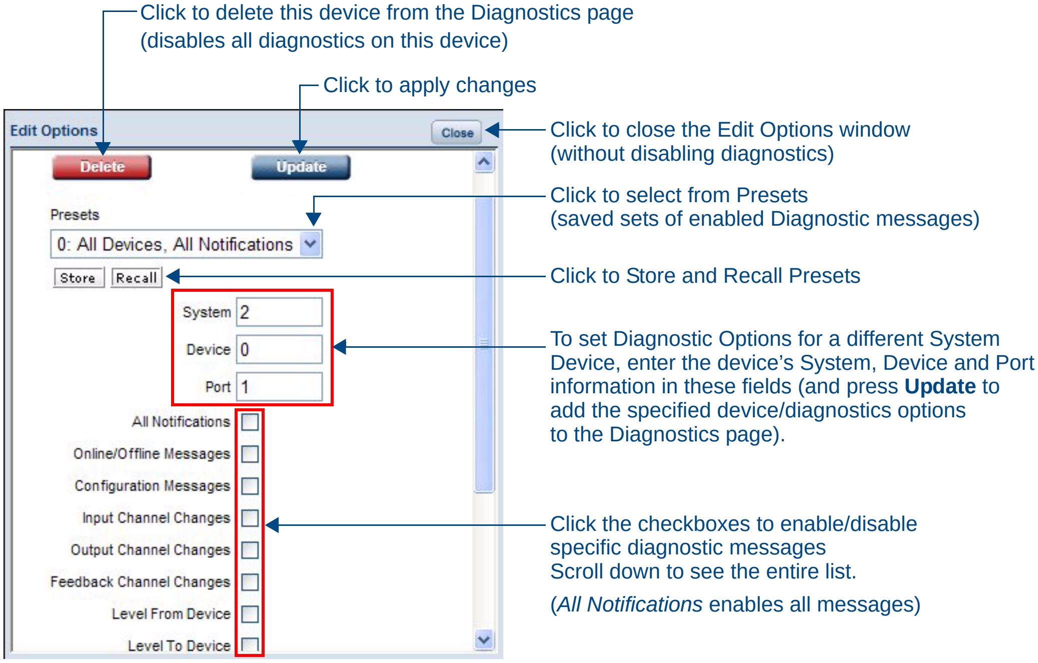
Copyright © 2006-2010 AMX LLC

FIG. 45 Select Diagnostics from within a selected Device's Network Settings page

***Note:** The currently selected device is also indicated in the **Device** field at the top of the page.*

2. By default, all diagnostics are disabled (see FIG. 45). To enable diagnostic messages from this device, click on one of the **Edit** buttons along the bottom of the Diagnostics Options table.

   This opens the Edit Options window (FIG. 46), where you can select which Diagnostics messages to enable or disable for this device.



Click to delete this device from the Diagnostics page (disables all diagnostics on this device)

Click to apply changes

Click to close the Edit Options window (without disabling diagnostics)

Click to select from Presets (saved sets of enabled Diagnostic messages)

Click to Store and Recall Presets

To set Diagnostic Options for a different System Device, enter the device's System, Device and Port information in these fields (and press **Update** to add the specified device/diagnostics options to the Diagnostics page).

Click the checkboxes to enable/disable specific diagnostic messages Scroll down to see the entire list.

(*All Notifications* enables all messages)

Edit Options

Close

Delete

Update

Presets

0: All Devices, All Notifications

Store Recall

System 2

Device 0

Port 1

All Notifications □

Online/Offline Messages □

Configuration Messages □

Input Channel Changes □

Output Channel Changes □

Feedback Channel Changes □

Level From Device □

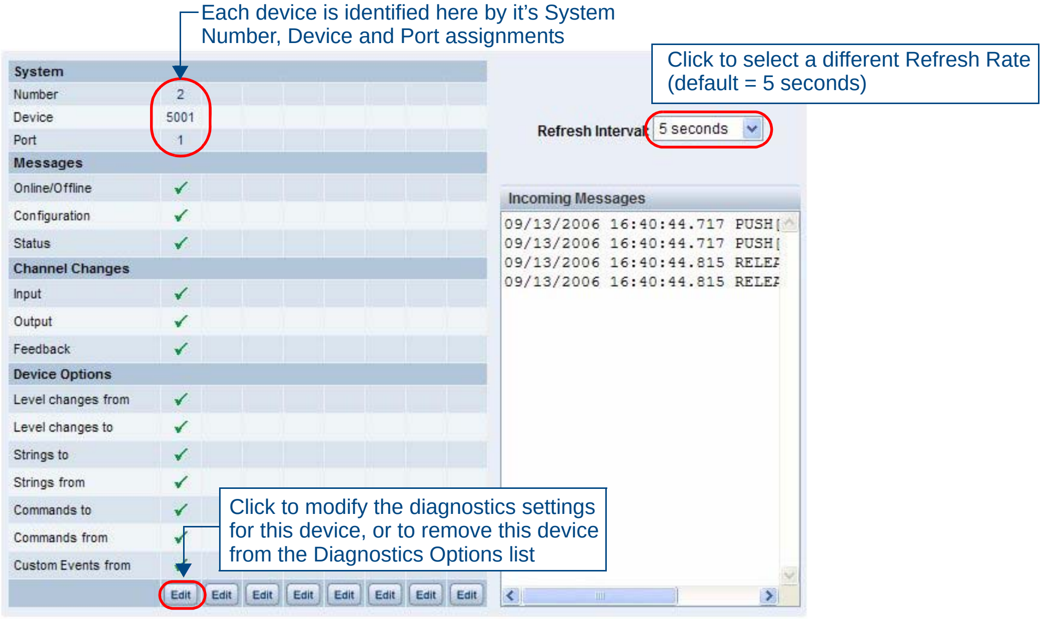
Level To Device □

FIG. 46 Edit Options window

Once you have selected the diagnostics messages to enable, click **Update** to apply your changes, close the Edit Options window, and return to the Diagnostics page.

Refer to the *Diagnostics Options Definitions* section on page 43 for definitions of each Diagnostic option.

3. The device that you just enabled diagnostics for appears in the Diagnostics Options page (identified by its Number, Device and Port assignments at the top of the Diagnostics Option list), with the currently enabled diagnostics indicated with a green check mark (FIG. 47).



Each device is identified here by it's System Number, Device and Port assignments

Click to select a different Refresh Rate (default = 5 seconds)

Click to modify the diagnostics settings for this device, or to remove this device from the Diagnostics Options list

System	
Number	2
Device	5001
Port	1
Messages	
Online/Offline	✓
Configuration	✓
Status	✓
Channel Changes	
Input	✓
Output	✓
Feedback	✓
Device Options	
Level changes from	✓
Level changes to	✓
Strings to	✓
Strings from	✓
Commands to	✓
Commands from	✓
Custom Events from	✓
	Edit

Refresh Interval 5 seconds

Incoming Messages

```
09/13/2006 16:40:44.717 PUSH[
09/13/2006 16:40:44.717 PUSH[
09/13/2006 16:40:44.815 RELEA
09/13/2006 16:40:44.815 RELEA
```

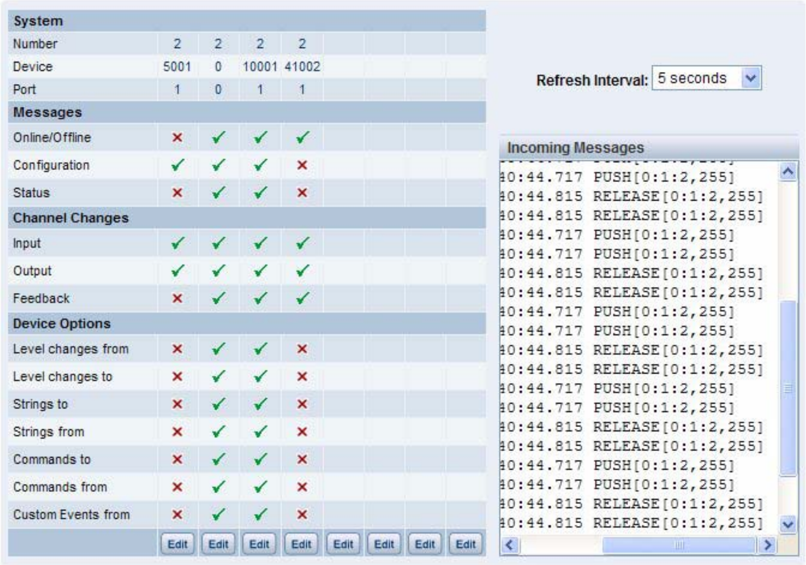
FIG. 47 Edit Options window

All returned messages are displayed in the Incoming Messages window. By default, all messages are refreshed every 5 seconds, as indicated by the **Refresh Interval** field. Use the Refresh Interval drop-down to specify how often your messages are updated (available values = 2 seconds, 5 seconds, or 10 seconds).

The default setting is 5 seconds.

4. To add more devices to the Diagnostics Options page:
    - Repeat steps 1-3.
    - Alternatively, you can click one of the **Edit** buttons to open the Edit Options window, and specify a System *Number*, *Device* and *Port* for a known System Device. Select the Diagnostics messages that you want to enable for this device and click **Update**.

      The device will appear in the Diagnostics Options window, in the next available column (to the right of the last device added - see FIG. 48).



System								
Number	2	2	2	2				
Device	5001	0	10001	41002				
Port	1	0	1	1				
Messages								
Online/Offline	✗	✓	✓	✓				
Configuration	✓	✓	✓	✗				
Status	✗	✓	✓	✗				
Channel Changes								
Input	✓	✓	✓	✓				
Output	✓	✓	✓	✓				
Feedback	✗	✓	✓	✓				
Device Options								
Level changes from	✗	✓	✓	✗				
Level changes to	✗	✓	✓	✗				
Strings to	✗	✓	✓	✗				
Strings from	✗	✓	✓	✗				
Commands to	✗	✓	✓	✗				
Commands from	✗	✓	✓	✗				
Custom Events from	✗	✓	✓	✗				
	Edit	Edit	Edit	Edit	Edit	Edit	Edit	Edit

Refresh Interval: 5 seconds

Incoming Messages

```
40:44.717 PUSH[0:1:2,255]
40:44.815 RELEASE[0:1:2,255]
40:44.815 RELEASE[0:1:2,255]
40:44.717 PUSH[0:1:2,255]
40:44.717 PUSH[0:1:2,255]
40:44.815 RELEASE[0:1:2,255]
40:44.815 RELEASE[0:1:2,255]
40:44.717 PUSH[0:1:2,255]
40:44.717 PUSH[0:1:2,255]
40:44.815 RELEASE[0:1:2,255]
40:44.815 RELEASE[0:1:2,255]
40:44.717 PUSH[0:1:2,255]
40:44.717 PUSH[0:1:2,255]
40:44.815 RELEASE[0:1:2,255]
40:44.815 RELEASE[0:1:2,255]
40:44.717 PUSH[0:1:2,255]
40:44.717 PUSH[0:1:2,255]
40:44.815 RELEASE[0:1:2,255]
40:44.815 RELEASE[0:1:2,255]
```

FIG. 48 Edit Options window indicating four devices with Diagnostics enabled

***Note:** You can monitor diagnostics for up to eight System Devices in this page.*

Diagnostics Options Definitions

The following table describes each of diagnostics options that can be enabled via the Edit Options window:

Diagnostic Options	
Diagnostic Option	Description
All Notifications:	Enables every notification field.
System	
• Number • Device • Port:	Use these fields to enter a Device:Port:System (D:P:S) combination for the device for which you want to enable notifications. A value of **0** for any option gives you all of the systems, devices, or ports. This dialog also allows you to store/recall presets.
Messages	
• Online/Offline	Generates a message when there is a change in the target device's online/offline status.
• Configuration	Generates a message when there is a change in the target device's configuration.
• Status	Generates a message when there is a change in the target device's status.
Channel Changes	
• Input	Generates a message when there is an input channel change (i.e. Push/Release) in the target device.
• Output	Generates a message when there is an output channel change (i.e. CHON/CHOFF) in the target device.
• Feedback	Generates a message when there is a feedback channel change in the target device.
Device Options	
• Level Changes From	Generates a message when there is a level channel change from the target device.
• Level Changes To	Generates a message when there is a level channel change to the target device.
• Strings To	Generates a message when there is a string sent to the target device.
• Strings From	Generates a message when there is a string from the target device.
• Commands To	Generates a message when there is a command to the target device.
• Commands From	Generates a message when there is a command from the target device.
• Custom Events From	Generates a message there is a custom event occurring from the target device.

Disabling all Diagnostic Options for a Device

There are two ways to disable all diagnostics for a device:

- In the Edit Options window, select **Delete** to remove the device from the Diagnostics Options page and disable all diagnostics.
- In the Edit Options window, clear all selected diagnostics options and click **Update**. This disables all diagnostics for this device, but leaves the device on the Diagnostics Options page.

Creating and Recalling Diagnostics Presets

The **Store** and **Recall** options in the Edit Options window allow you to save and recall preset diagnostics configurations.

Note: *Presets are saved via cookies, so they do not persist across multiple browsers/computers.*

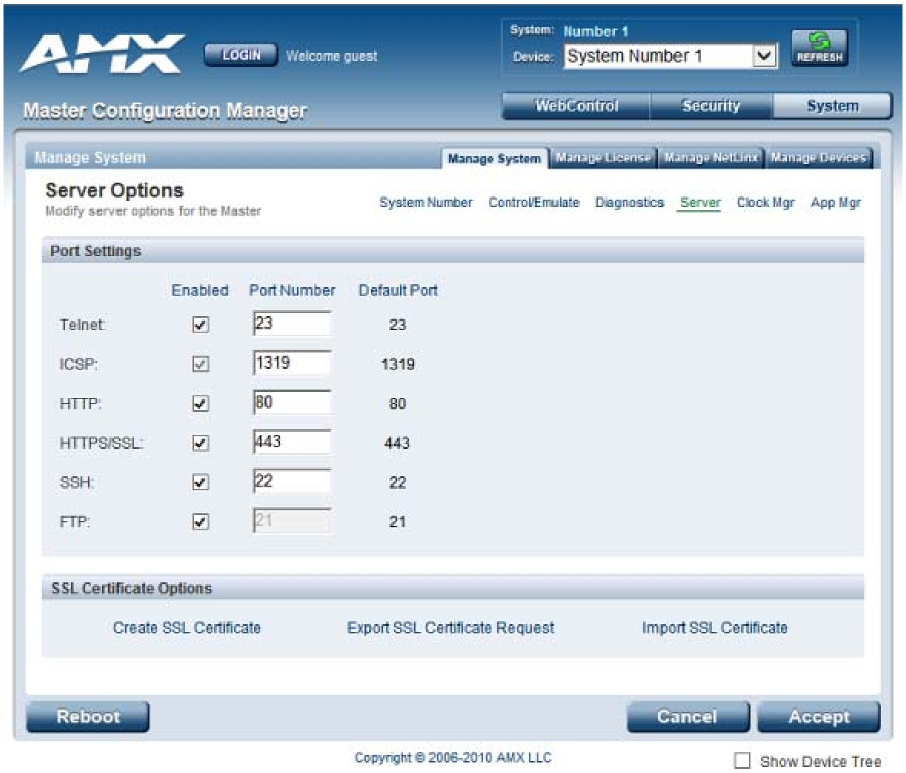
1. Click the **Presets** down arrow to open a list of previously stored Presets. By default, the only preset is called **0: All Devices, All Notifications**. This default Preset cannot be modified.
2. Select an empty Preset (for example **1:**)
3. Select the desired diagnostic options, and click **Store**.
4. A popup window prompts you to name this Preset. Enter a name and click **OK**. To recall an existing Preset, select it from the drop-down list and click on **Recall**.

Note: *A Preset MUST be Recalled before clicking the Update button. If you do not press this button, none of the fields or checkboxes are modified or selected. In essence, all options become disabled.*

Manage System - Server Options

Click the **Server** link (in the *Manage System* tab) to access the Server Options page (FIG. 49). The options on this page allow you to:

- Change the port numbers (used by the Master for various Web services)
- Configure the SSL settings used on the Master
- Manage existing and pending license keys, manage the active NetLinx system communication parameters
- Configure/modify the SSL certificates on the target Master



Server Options
Modify server options for the Master

Port Settings

	Enabled	Port Number	Default Port
Telnet:	☑	23	23
ICSP:	☑	1319	1319
HTTP:	☑	80	80
HTTPS/SSL:	☑	443	443
SSH:	☑	22	22
FTP:	☑	21	21

SSL Certificate Options

FIG. 49 Server Options page

The options on this page are described below:

Port Settings

Allows a user to modify the server settings; specifically those port assignments associated with individual services.

- All items can be either enabled/disabled via the **Enabled** checkboxes.
- The port number values (except the FTP port) can be modified in this page.
- The default port for each service is listed to the right.

Server Port Settings

The following table describes each of the Port Settings presented on this page:

Server Port Settings	
Feature	Description
Telnet:	The port value used for Telnet communication to the target Master. Enabling this feature allows future communication with the Master via a separate Telnet application (such as HyperTerminal). • The default port value is **23**. • Refer to the *NetLinx Security with a Terminal Connection* section for more information on the related procedures.
ICSP:	The port value used for ICSP data communication among the different AMX software and hardware products. This type of communication is used by the various AMX product for communication amongst themselves. Some examples would be: NetLinx Studio communicating with a Master (for firmware or file information updates) and TPDesign4 communicating with a touch panel (for panel page and firmware updates). • The default port value is **1319**. ***Note****: To further ensure a secure connection within this type of communication, a user can enable the Require Encryption option which requires additional processor cycles. Enabling of the encryption feature is determined by the user.*
HTTP:	The port value used for unsecure HTTP Internet communication between the web browser's UI and the target Master. By disabling this port, the administrator (or other authorized user) can require that any consecutive sessions between the UI and the target Master are done over a more secure HTTPS connection. By default, the Master does not have security enabled and must be communicated with using **http://** in the *Address* field. • The default port value is **80**. ***Note****: One method of adding security to HTTP communication is to change the Port value. If the port value is changed, any consecutive session to the target Master has to add the port value at the end of the address (within the Address field). An example is if the port were changed to 99, the new address information would be:* ***http://192.192.192.192:99****.*
HTTPS/SSL:	The port value used by web browser to securely communicate between the web server UI and the target Master. This port is also used to simultaneously encrypt this data using the SSL certificate information on the Master as a key. This port is used not only used to communicate securely between the browser (using the web server UI) and the Master using HTTPS but also provide a port for use by the SSL encryption key (embedded into the certificate). Whereas SSL creates a secure connection between a client and a server, over which any amount of data can be sent securely, HTTPS is designed to transmit individual messages securely. Therefore both HTTPS and SSL can be seen as complementary and are configured to communicate over the same port on the Master. These two methods of security and encryption are occurring simultaneously over this port as data is being transferred. • The default port value is **443**. ***Note****: Another method of adding security to HTTPS communication would be to change the port value. If the port value is changed, any consecutive session to the target Master has to add the port value at the end of the address (within the Address field). An example is if the port were changed to 99, the new address information would be:* ***http://192.192.192.192:99****.*

Server Port Settings (Cont.)	
Feature	Description
SSH:	• The port value used for secure Telnet communication. A separate secure SSH Client would handle communication over this port. When using a secure SSH login, the entire login session (including the transmission of passwords) is encrypted; therefore it is secure method of preventing an external user from collecting passwords. • SSH **version 2** is supported. • The default port value is **22**. ***Note**: If this port's value is changed, make sure to use it within the Address field of the SSH Client application.*
FTP:	The default port value used for FTP communication = 21. ***Note**: This port can be disabled/enabled but the value can not be changed.*

Once any of the server port settings have been modified, press the **Accept** button to save these changes to the Master. Once these changes are saved, the following message appears: *"Unit must be rebooted for the change to take effect"*.

Click the **Reboot** button (*from the top of the page*) to remotely reboot the target Master. No dialog appears while using this button. The Device Tree then reads *"Rebooting...."*. After a few seconds, the Device Tree refreshes with the current system information (indicating updated port numbers).

***Note:** If the Device Tree contents do not refresh within a few minutes, press the browser's Refresh button and reconnect to the Master.*

SSL Certificate Options

There are three SSL Certificate options, presented as links along the bottom of this page:

SSL Certificate Options	
Create SSL Certificate:	Opens the Create SSL Certificate window where you can create a self-generated SSL certificate. **Note**: A self-generated certificate has lower security than an external CA (officially issued) generated certificate.
Export SSL Certificate Request:	Takes the user to the Server Certificate page where they can view a previously created certificate. An authorized user can also copy the raw text from a generated Certificate request into their clipboard and then send it to the CA.
Import SSL Certificate:	Takes the user to the Import Certificate page where they can import and paste the raw text from a CA issued Certificate.

Creating an SSL Server Certificate

Initially, a NetLinx Master is not equipped with any installed certificates. To prepare a Master for later use with "CA" (*officially issued*) server certificates, it is necessary to:

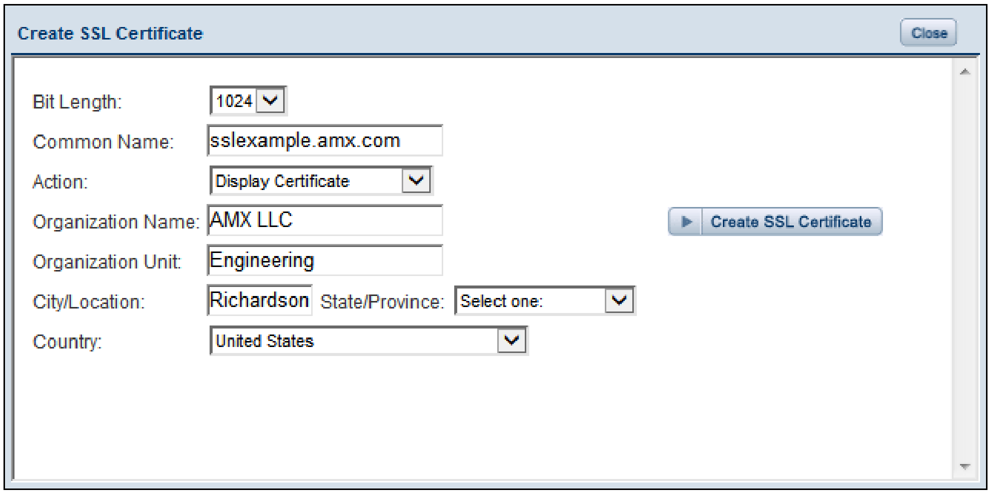
- **First create a self-generated certificate** which is automatically installed onto the Master.
- **Secondly, enable the SSL feature** from the Enable Security page. Enabling SSL security after the certificate has been self-generated insures that the target Master is utilizing a secure connection during the process of importing a CA server certificate over the web.

***Note:** A certificate consists of two different Keys:*

*The **Master Key** is generated by the Master and is incorporated into the text string sent to the CA during a certificate request. It is unique to a particular request made on a specific Master. Note that regenerating a previously requested and installed certificate invalidates that certificate because the Master Key has been changed.*

*The **Public Key** is part of the text string that is returned from the CA as part of an approved SSL Server Certificate. This public key is based off the submitted Master key from the original request.*

1. Click the **Create SSL Certificate** link (under *SSL Certificate Options*) to access the *Create SSL Certificate* window (FIG. 50).



Bit Length: 1024

Common Name: sslexample.amx.com

Action: Display Certificate

Organization Name: AMX LLC

Organization Unit: Engineering

City/Location: Richardson State/Province: Select one:

Country: United States

FIG. 50 Create SSL Certificate window

2. Fill out the information in this window, according to the descriptions in the *SSL Certificate Entries* section below.
3. Click **Create SSL Certificate** to update the Master with the information entered on this page. This process can take several minutes.

SSL Certificate Entries

The following table describes the SSL Certificate entries presented in the *Create SSL Certificate* window (FIG. 50):

SSL Certificate Entries	
Entry	Description
Bit Length:	Provides a drop-down selection with three public key lengths (512, 1024, 2048). • A longer key length results in more secure certificates. • Longer key lengths result in increased certificate processing times.
Common Name:	The Common Name of the certificate must match the URL Domain Name used for the Master. Example: If the address used is www.amxuser.com, that must be the Common name and format used. • The Common Name can not be an IP Address. • If the server is internal, the Common Name must be *Netbios*. • For every website using SSL that has a distinct DNS name, there must be a certificate installed. Each website for SSL must also have a distinct IP Address. • This domain name must be associated to a resolvable URL Address when creating a request for a purchased certificate. • The address does not need to be resolvable when obtaining a free certificate.
Action:	Provides a drop-down selection with a listing of certificate actions: • **Display Certificate** - Populates the Server Certificate fields with the information from the certificate currently installed on the Master. *This action is used only to display the information contained in the certificate on the target Master.* • **Create Request** - Takes the information entered into these fields and formats the certificate so it can be exported to the external Certificate Authority (CA) for later receipt of an SSL Certificate. *This action is used to request a certificate from an external source.* • **Self Generate Certificate** - Takes the information entered into the previous fields and generates its own SSL Certificate. *This action is used when no previous certificate has been installed on the target Master, or a self-signed certificate is desired.* • **Regenerate Certificate** - Takes the information entered into the previous fields and regenerates an SSL Certificate. This action changes the Master Key. *This method of certificate generation is used to modify or recreate a previously existing certificate already on the Master.*
Organization Name:	Name of your business or organization. This is an alpha-numeric string (1 - 50 characters in length).
Organization Unit:	Name of the department using the certificate. This is an alpha-numeric string (1 - 50 characters in length).
City/Location:	Name of the city where the certificate is used. This is an alpha-numeric string (1 - 50 characters in length).
State/Province:	Name of the state or province where the certificate is used (alpha-numeric string, 1 - 50 characters in length). ***Note****: The state/province name must be fully spelled out.*
Country Name:	Provides a drop-down selection with a listing of currently selectable countries.

Displaying SSL Server Certificate Information

Click the *Create SSL Certificate* link in the Server Options page to open the Create SSL Certificate window.

- By default, the *Display Certificate* Action is selected and the fields in this window are populated with information from the certificate installed on the Master.
- If the Master does not have a previously installed certificate, these fields are blank.

Creating a Request for an SSL Certificate

1. Click the *Create SSL Certificate* link in the Server Options page to open the *Create SSL Certificate* window.
2. Fill out the fields, according to the descriptions in the *SSL Certificate Entries* section on page 48.
3. Click the down arrow next to the *Action* field, and choose **Create Request** from the drop-down list.
4. Click the **Create SSL Certificate** button to accept the information entered into the above fields and generate a certificate file. Click **Close** to exit without making changes to the Master. This refreshes the Server Certificate page, and if the certificate request was successful, displays a *"Certified request generated"* message.

Self-Generating an SSL Certificate

1. Click the *Create SSL Certificate* link in the Server Options page to open the Create SSL Certificate window.
2. Fill out the fields, according to the descriptions in the *SSL Certificate Entries* section on page 48.
3. Click the down arrow next to *Action* and choose **Self Generate Certificate**.

   When this request is submitted, the certificate is generated and installed into the Master in one step.
4. Click **Create SSL Certificate** to save the new encrypted certificate information to the Master. Click **Close** to exit without making changes to the Master.

Regenerating an SSL Server Certificate Request

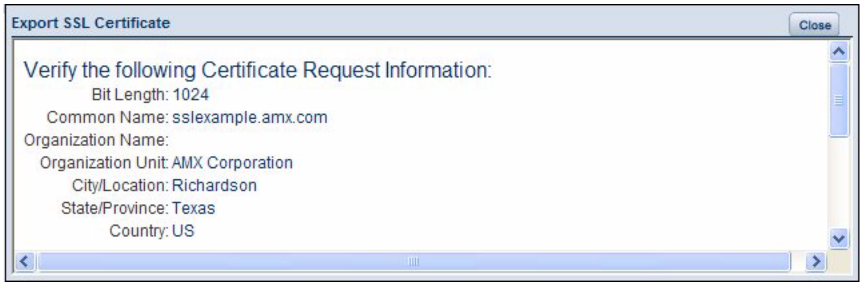
This action allows you to is used to modify or recreate a certificate already on the Master. For example, if the company has moved from Dallas to Houston, all of the information is reentered exactly except for the City.

1. Click the **Create SSL Certificate** link in the *Server Options* page to open the *Create SSL Certificate* window.
2. Modify the certificate information as needed (see the *SSL Certificate Entries* section on page 48).
3. Click the down arrow next to *Action* and choose **Regenerate Certificate**.
4. Click **Create SSL Certificate** to save the newly modified certificate information to the Master. Click **Close** to exit without making changes to the Master.

CAUTION!: *Only use the **Regenerate Certificate** option when you have self-generated your own certificate. Do not regenerate an external CA-generated certificate.*

Exporting an SSL Certificate Request

1. First follow the procedures outlined in the *Creating a Request for an SSL Certificate* section on page 49 to create a session-specific Master certificate.
2. Click the **Export SSL Certificate** link to display the certificate text file in the Export SSL Certificate window (FIG. 51).



Verify the following Certificate Request Information:
Bit Length: 1024
Common Name: sslexample.amx.com
Organization Name:
Organization Unit: AMX Corporation
City/Location: Richardson
State/Province: Texas
Country: US

FIG. 51 Export SSL Certificate window

3. Place your cursor within the certificate text field.

   The certificate text begins with the line that reads "-----BEGIN CERTIFICATE REQUEST-----" (scroll down to view the certificate text.)
4. Select all (**Ctrl** + **A**) of the certificate text.

   You must copy all of the text within this field, including the **-----BEGIN CERTIFICATE REQUEST-----** and the **-----END CERTIFICATE REQUEST-----** portions.

   Without this text included in the CA submission, you will not receive a CA-approved certificate.
5. Copy (**Ctrl** + **C**) the text to the clipboard.
6. Paste (**Ctrl** + **V**) this text into the *Submit Request* field on the CA's Retrieve Certificate web page.

7. Choose to view the certificate response in raw DER format.

   Note the **Authorization Code** and **Reference Number** (for use in the e-mail submission of the request).

8. Submit the request.

9. Paste the copied text into your e-mail document and send it to the CA with its accompanying certificate application.

WARNING!: *When a certificate request is generated, you are creating a private key on the Master.*

You can not request another certificate until the previous request has been fulfilled.

Doing so voids any information received from the previously requested certificate and it becomes nonfunctional if you try to use it.

Once you have received the returned CA certificate, follow the procedures outlined in the following section to import the returned certificate (*over a secure connection*) to the target Master.

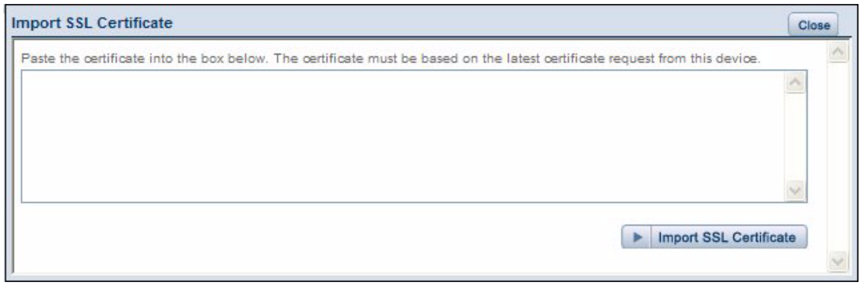
Importing an SSL Certificate

Click the **Import SSL Certificate** link to import a CA server certificate. Before importing an SSL Certificate you must:

- **First**, have a self-generated certificate installed onto your target Master.
- **Second**, enable the *HTTPS/SSL* feature from the Server Options page (FIG. 49), to establish a secure connection to the Master prior to importing the encrypted CA certificate.

1. Copy the returned certificate (signed by the CA) to your clipboard.

2. Click the *Import SSL Certificate* link to open the Import SSL Certificate window (FIG. 52).



Import SSL Certificate

Paste the certificate into the box below. The certificate must be based on the latest certificate request from this device.

FIG. 52 Import SSL Certificate window

3. Place the cursor inside the text box and paste the returned certificate text, in its entirety.

4. Click **Import SSL Certificate** to save the new certificate information to the Master.

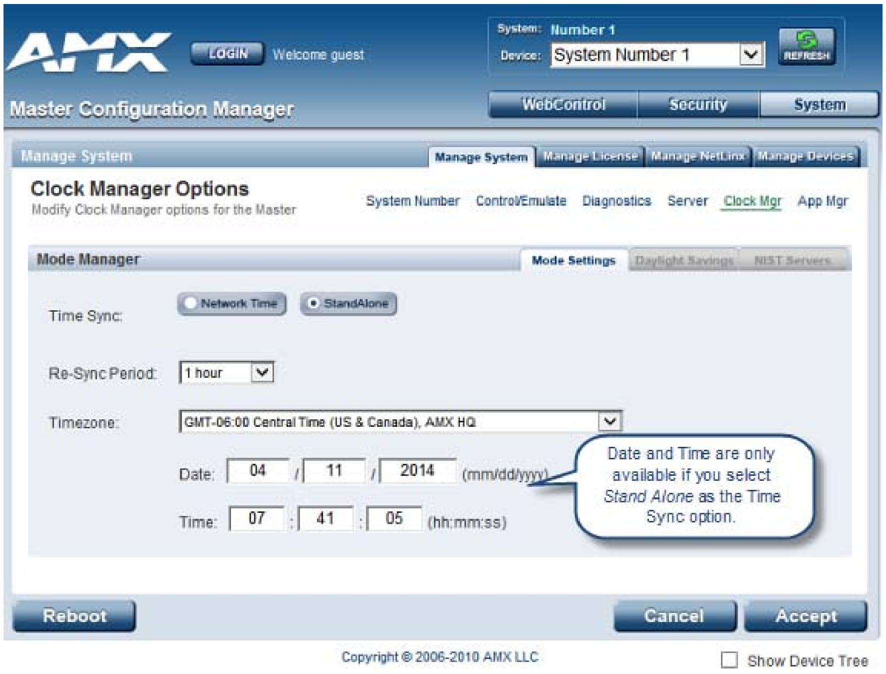
CAUTION!: *Once a certificate has been received from an external CA and installed on a Master, do not regenerate the certificate or alter its properties. Regenerating a previously installed certificate, invalidates the certificate.*

5. Click the **Display Certificate** link to confirm the new certificate was imported properly to the target Master.

Note: *A CA certificate can only be imported to a target Master only after both a self-generated certificate has been created and the SSL Enable feature has been selected on the Master. These actions configure the Master the secure communication necessary during the importing of the CA certificate.*

Manage System - Clock Manager Options

Click the **Clock Mgr** link (on the *Manage System* tab) to access the *Clock Manager Options* page (FIG. 53). The options on this page allow you to enable/disable using a network time source and provide access to Daylight Saving configuration and which NIST servers to use as a reference.



System: Number 1

Device: System Number 1

Clock Manager Options

Modify Clock Manager options for the Master

Time Sync: ○ Network Time ● StandAlone

Re-Sync Period: 1 hour

Timezone: GMT-06:00 Central Time (US & Canada), AMX HQ

Date: 04 / 11 / 2014 (mm/dd/yyyy)

Time: 07 : 41 : 05 (hh:mm:ss)

Date and Time are only available if you select *Stand Alone* as the Time Sync option.

Copyright © 2006-2010 AMX LLC

□ Show Device Tree

FIG. 53 Clock Manager Options - Mode Settings tab

The Clock Manager Options are separated into three tabs:

- **Mode Settings** - The Mode Manager in this tab allows you to set the Clock Manager Mode (Network Time or Stand Alone).
- **Daylight Savings** - The Daylight Savings Manager in this tab allows you to specify how and when to implement Daylight Savings rules on the clock.
- **NIST Servers** - The NIST Server Manager in this tab allows you to connect to a specific NIST (Internet Time Service) Server.

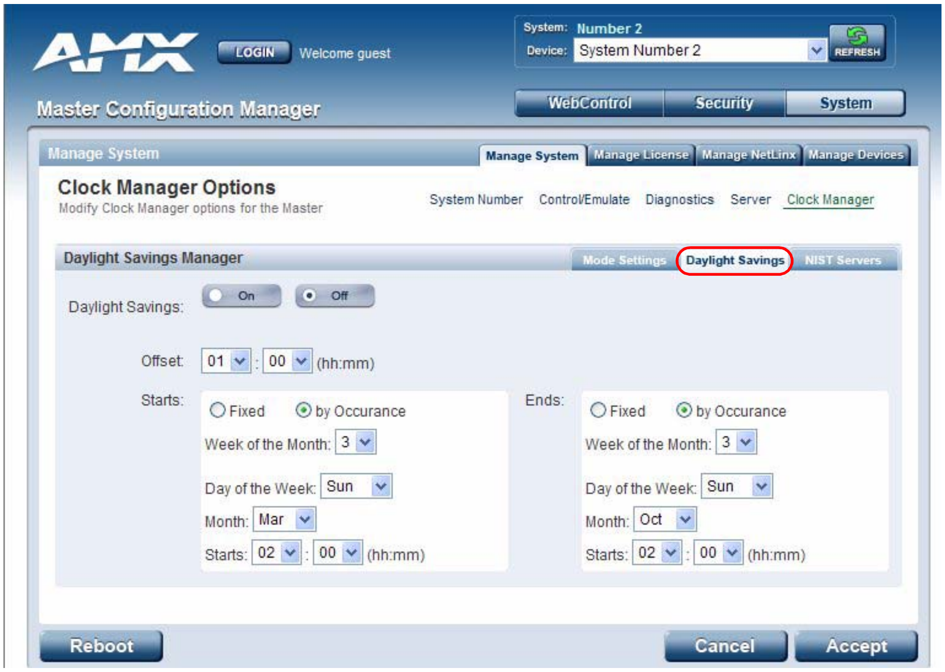
Setting the Mode for the Clock Manager

1. In the *Manage System* tab (FIG. 53), select a **Time Sync** option.
   - **Network Time**: This option allows the Master to manage it’s clock by connecting to a NIST (Internet Time Service) Server. When this option is selected, the Master will connect to the default NIST Server to get date and time information.

     You can select a different NIST Server (or specify the IP Address of a known NIST Server) in the *NIST Servers* tab (see the *Selecting a Custom NIST Server* section on page 53).
   - **Stand Alone**: This option lets the Master use its own internal clock. When this option is selected, two additional fields are available on this tab:
     - **Date** - Enter the current date in these fields (mm/dd/yyyy).
     - **Time** - Enter the current time in these fields (hh/mm/ss).
2. Click **Accept** to save these settings to the Master.

Setting Daylight Savings Rules

1. In the *Daylight Savings* tab (FIG. 54), enable Daylight Savings mode by clicking the **On** button.



Daylight Savings: ○ On ● Off

Offset: 01 : 00 (hh:mm)

Starts: ○ Fixed ● by Occurance

Week of the Month: 3

Day of the Week: Sun

Month: Mar

Starts: 02 : 00 (hh:mm)

Ends: ○ Fixed ● by Occurance

Week of the Month: 3

Day of the Week: Sun

Month: Oct

Starts: 02 : 00 (hh:mm)

FIG. 54 Clock Manager Options - Daylight Savings tab

2. Use the **Offset** drop-down menus to adjust the amount of time (hours and minutes) to offset Daylight Savings. By default, the offset is set to 1 hour.

***Note:** Although most places that support Daylight Savings usually adjust the local time by one hour this doesn't cover all locations. To provide flexibility for such locations it is possible to configure a different daylight savings time offset.*

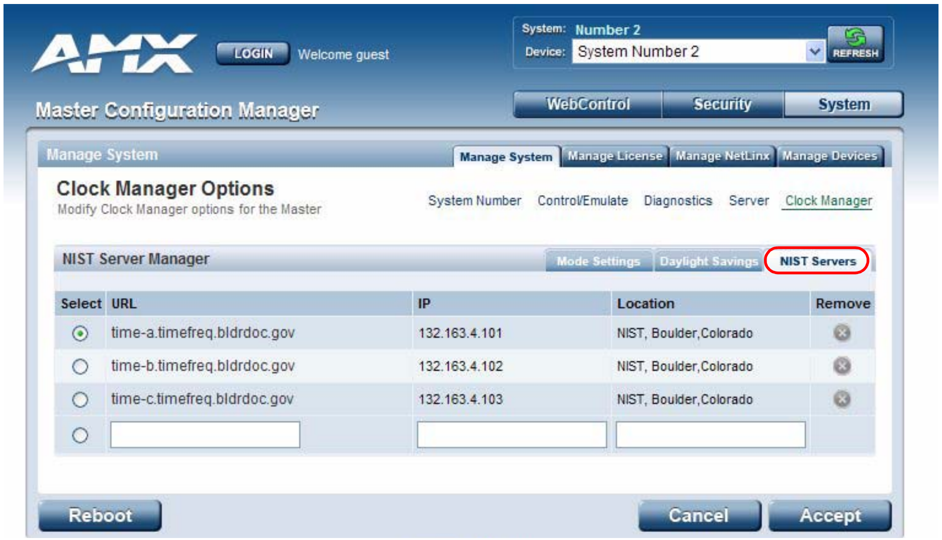
3. Use the **Starts** fields to specify when Daylight Savings should start. The Starts rules include:
   - Select **Fixed** to specify the calendar date when the rule applies as a specific date ("March 21"). When *Fixed* is selected, use the **Day**, **Month** and **Starts** fields to specify the date and time (hh:mm) to start Daylight Savings time.
   - Select **by Occurrence** to specify the calendar date when the rule applies as a heuristic, ("the 3rd Sunday in March"). When *by Occurrence* is selected, use the **Week of the Month**, **Day of the Week**, **Month** and **Starts** fields to specify the occurrence to start Daylight Savings time.

     The range is 1 through *Last*, where **Last** indicates the last occurrence of a particular day of the month. This is to accommodate months that include four weeks as well as those that include five.

4. Use the **Ends** fields to specify when Daylight Savings should end. The Ends rules match the Start rules, and follow the same logic. Select **Fixed** or **by Occurrence**, and specify the End date/time information accordingly.

5. Click **Accept** to save these settings to the Master.

Selecting a Custom NIST Server



Select	URL	IP	Location	Remove
●	time-a.timefreq.bldrdoc.gov	132.163.4.101	NIST, Boulder,Colorado	⊗
○	time-b.timefreq.bldrdoc.gov	132.163.4.102	NIST, Boulder,Colorado	⊗
○	time-c.timefreq.bldrdoc.gov	132.163.4.103	NIST, Boulder,Colorado	⊗
○				

FIG. 55 Clock Manager Options - NIST Servers tab

1. In the *NIST Servers* tab (FIG. 55), use the radio buttons to select one of the NIST Servers in the list.
2. Click **Accept** to save these settings to the Master.

Adding a Custom NIST Server to the List

1. Click on the radio button next to the last (blank) entry in the *NIST Server Manager* list.
2. In the **URL** field, enter the URL of the NIST Server. The URL is used only to help you manage entries, and is not verified or used internally by the clock manager.
3. Enter the NIST Server's IP Address in the **IP** field. This is used internally and must be a valid IP address.

***Note:** The strings entered into the URL and Location fields are not used to connect to NIST Servers. The IP Address (entered into the **IP** field) specifies the NIST Server(s) that will be used. As stated above, the address entered into the **IP** field must be must be a valid IP address (not a URL).*

4. Enter the NIST Server's location in the **Location** field. This is used only to help the user manage entries and it is not verified or used internally by the clock manager.
5. Click **Accept** to save these settings to the Master.

Removing an NIST Server From the List

1. Click on the **Remove** (x) button to the right of a *user-added* NIST Server in the *NIST Server Manager* list.
2. Click **Accept** to save these settings to the Master.

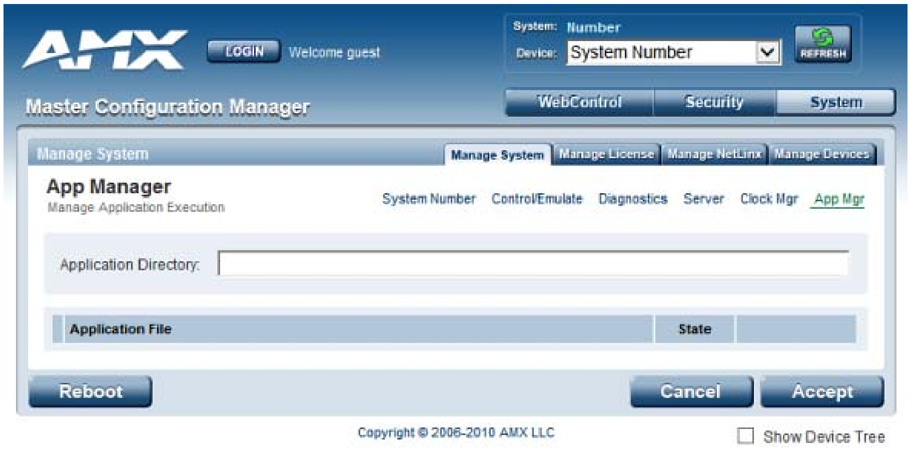
***Note:** The built-in entries cannot be removed.*

Clock Manager NetLinx Programming API

Refer to *Appendix C: Clock Manager NetLinx Programming API* section on page 145 for a listing and description of the Types/Constants and Library Calls that are included in the NetLinx.AXI to support Clock Manager functions.

Manage System - App Manager Options

Click the **App Mgr** link (on the *Manage System* tab) to access the *App Manager Options* page (FIG. 56). The options on this page allow you to specify a directory location on the Master where you want to store Java applications used by the Master and then manage the applications, including installing, starting, stopping, and deleting them.



System: Number

Device: System Number

App Manager

Manage Application Execution

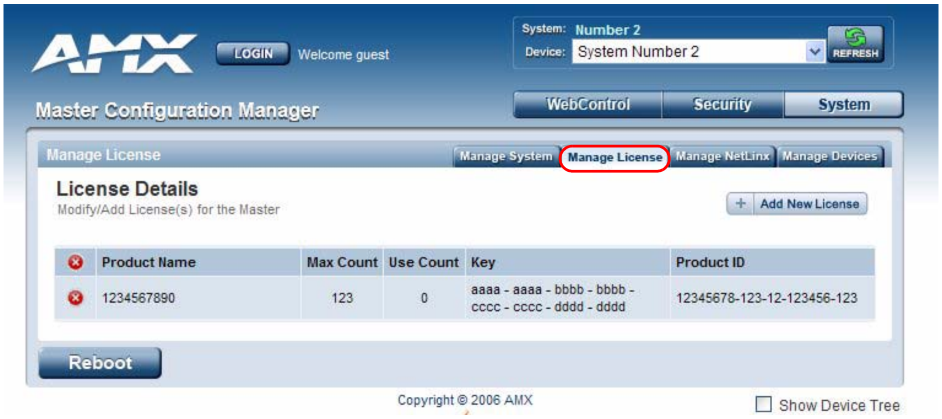
Application Directory:

Application File	State

FIG. 56 App Manager options

System - Manage License

The **Manage License** tab displays current as well as pending license keys (FIG. 57).



System: Number 2

Device: System Number 2

License Details

Modify/Add License(s) for the Master

	Product Name	Max Count	Use Count	Key	Product ID
⊗	1234567890	123	0	aaaa - aaaa - bbbb - bbbb - cccc - cccc - dddd - dddd	12345678-123-12-123456-123

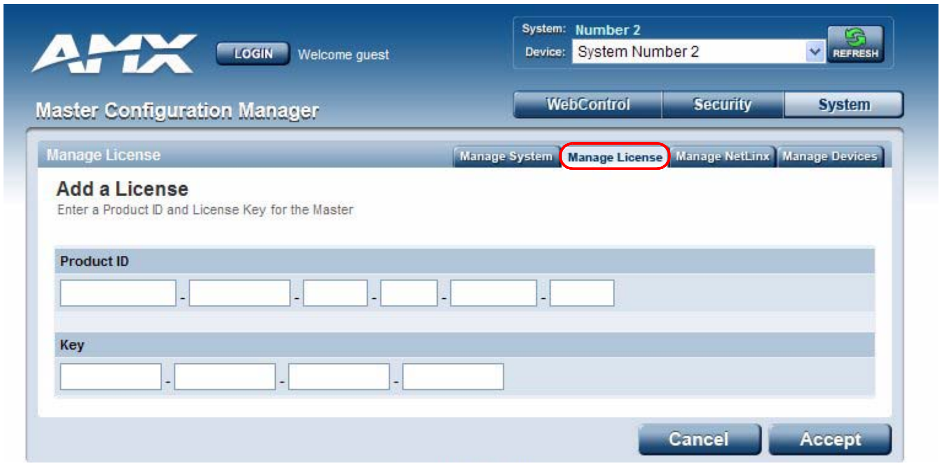
FIG. 57 System - Manage License tab (with one example entry)

The **Add New License** button allows for the addition of new license keys associated with currently used modules/ products. Adding new License Keys requires the entry of both a Product ID and a Serial Key (example: *i!-Voting)*.

The Master confirms this registration information before running the module or product.

Adding a New License

1. Click the **Add New License** button to access the *Add a License* page (FIG. 58).



Add a License

Enter a Product ID and License Key for the Master

Product ID

Key

FIG. 58 Manage License - Add a License page

2. Enter the Product ID (certificate number) provided with the product into the **Product ID** fields.

   Contact the AMX Sales department with both the product serial number (or certificate number) and the serial number of target Master to register your product and in turn receive the necessary Key information (typically 32 to 36 digits in length) which is then entered into the Key fields on this page.

3. Enter the Product Key into the **Key** fields. The Product Key is Master-specific and is typically provided by AMX upon registration.

   Example: *AMX Meeting Manager* and *i!-Voting* applications are examples of products that require both a Product serial number and a Master-specific key prior to usage.

4. Press the **Accept** button to save the information. If there are no errors with the information on this page, a "*Key successfully added for Product ID XXXX*" is displayed at the top of the page.

Removing a License

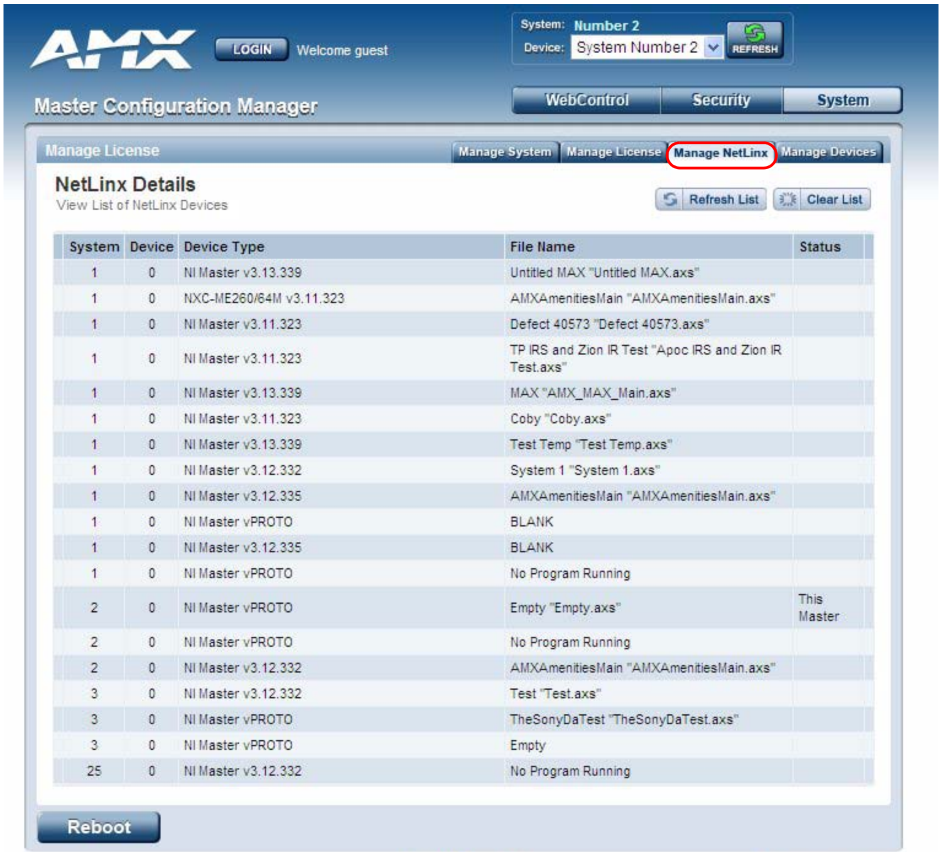
1. Click the **Remove** (x) icon to the left of the license that you want to remove.

2. The system will prompt you to verify this action before the license is removed from the Master. Click **OK** to proceed.

3. Press the **Accept** button to save the information.

System - Manage NetLinx

The **Manage NetLinx** tab displays a list of NetLinx devices connected to the Master, and indicates device status for each (FIG. 59).



NetLinx Details

View List of NetLinx Devices

System	Device	Device Type	File Name	Status
1	0	NI Master v3.13.339	Untitled MAX "Untitled MAX.axs"	
1	0	NXC-ME260/64M v3.11.323	AMXAmenitiesMain "AMXAmenitiesMain.axs"	
1	0	NI Master v3.11.323	Defect 40573 "Defect 40573.axs"	
1	0	NI Master v3.11.323	TP IRS and Zion IR Test "Apoc IRS and Zion IR Test.axs"	
1	0	NI Master v3.13.339	MAX "AMX_MAX_Main.axs"	
1	0	NI Master v3.11.323	Coby "Coby.axs"	
1	0	NI Master v3.13.339	Test Temp "Test Temp.axs"	
1	0	NI Master v3.12.332	System 1 "System 1.axs"	
1	0	NI Master v3.12.335	AMXAmenitiesMain "AMXAmenitiesMain.axs"	
1	0	NI Master vPROTO	BLANK	
1	0	NI Master v3.12.335	BLANK	
1	0	NI Master vPROTO	No Program Running	
2	0	NI Master vPROTO	Empty "Empty.axs"	This Master
2	0	NI Master vPROTO	No Program Running	
2	0	NI Master v3.12.332	AMXAmenitiesMain "AMXAmenitiesMain.axs"	
3	0	NI Master v3.12.332	Test "Test.axs"	
3	0	NI Master vPROTO	TheSonyDaTest "TheSonyDaTest.axs"	
3	0	NI Master vPROTO	Empty	
25	0	NI Master v3.12.332	No Program Running	

FIG. 59 System - Manage NetLinx tab

The table on this page consists of five columns:

NetLinx Device Details	
Column	Description
System:	Displays the System value being used by the listed NetLinx Master.
Device:	Displays the assigned device value of the listed unit. This Device entry applies to both the Master and those NDP-capable devices currently connected to that Master.
Device Type:	Displays a description of the target Master or connected device, and its current firmware version. Example: *NI Master v3.01.323*.
File Name:	Displays the program name and/or file resident on the device.
Status:	Indicates the Master or device state: • **This Master**: Indicates its the target Master currently being used and being browsed to. Its this Master's web pages which are currently being viewed. • **Orphan**: Indicates that the device is currently not yet "bound" or assigned to communicate with a particular Master. This state shows an adjacent **Bind** button which is used to bind the device to the Master whose web pages are currently being viewed. • **Searching**: Indicates that the device is trying to establish communication with it's associated Master. • **Bound**: Indicates that the device has established communication with it's associated Master. This state shows an adjacent **Unbind** button which is used to release/disassociate the device from communicating with its current Master. • **Lost**: Indicates that the device has tried to establish communication with it's associated or "bound" Master, but was after a period of time, unable to establish communication.

- **Refresh List**: Click this button to regenerate the device listing by looking for broadcasting devices. This causes the Master to send out a message asking devices to resend their NDP device announcements. The list is then updated as those devices send back their announcements to the Master.

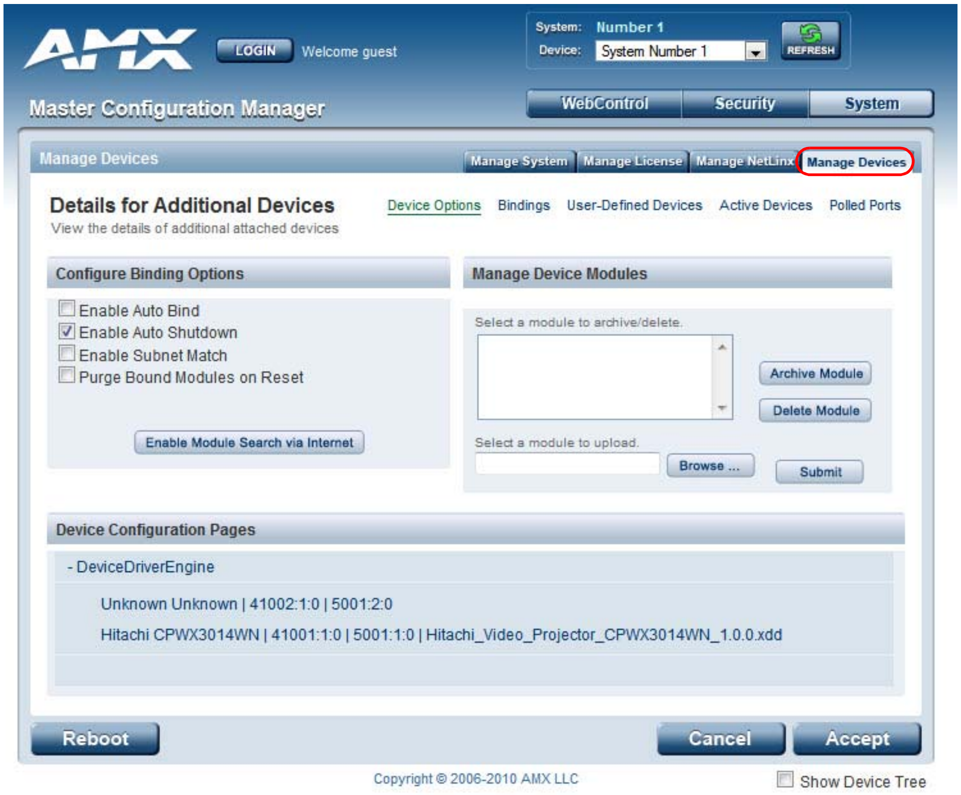
  The information displayed can not only include Masters and devices on this system but Masters and devices on other systems as well. By default, the target Master always appears in the list.

***Note:** Due to system delays, message collisions, and multicast routing, not all devices may respond immediately.*

- **Clear List**: Click this button causes the entries to be temporarily deleted from the page, either until you refresh the list (using the *Refresh List* button), or until the Master begins to detect any multi-cast transmissions from System Devices.

System - Manage Devices

The **Manage Devices** tab (FIG. 60) contains links to several different device-related pages, as described in the following subsections.


LOGIN
Welcome guest
REFRESH
Master Configuration Manager
WebControl
Security
System
Manage Devices
Manage System
Manage License
Manage NetLinx
Manage Devices
Details for Additional Devices
View the details of additional attached devices
Device Options
Bindings
User-Defined Devices
Active Devices
Polled Ports
Configure Binding Options
Manage Device Modules
Select a module to archive/delete.
Archive Module
Delete Module
Select a module to upload.
Browse ...
Submit
Enable Module Search via Internet
Device Configuration Pages
Reboot
Cancel
Accept
Copyright © 2006-2010 AMX LLC

System: Number 1

Device: System Number 1

□ Enable Auto Bind

☑ Enable Auto Shutdown

□ Enable Subnet Match

□ Purge Bound Modules on Reset

- DeviceDriverEngine

Unknown Unknown | 41002:1:0 | 5001:2:0

Hitachi CPWX3014WN | 41001:1:0 | 5001:1:0 | Hitachi_Video_Projector_CPWX3014WN_1.0.0.xdd

□ Show Device Tree

FIG. 60 System - Manage Devices (Details for Additional Devices)

Manage Devices - Device Options

Click the **Device Options** link (in the *Manage Devices* tab) to access the **Details for Additional Devices** page (FIG. 60). The options on this page display various details specific to additional (non-NetLinx) System Devices.

Configuring Device Binding Options

1. Use the **Configure Binding Options** options to specify how the Master will manage Bound Devices:

Binding Options	
Option	Description
Enable Auto Bind:	This selection allows you to toggle the state of the automatic binding for DDD (On/Off). When auto-binding is enabled, the Master automatically attempts to connect any newly discovered device with an associated application device (defined in the running NetLinx application). Auto-binding can only be accomplished if the Master's firmware determines a one-to-one correlation between the newly discovered device and a single entry within the list of defined application devices (accessed via the *Binding* link at the top of this page). For example, if the application only has one VCR defined and a VCR is detected in the system, auto-binding can then be accomplished. If there were two VCRs defined within the application, auto-binding could not be completed due to the lack of a clearly defined one-to-one correspondence. When this option is not selected, no auto-binding activity takes place and all binding of the newly discovered devices must be accomplished manually via the Web control interface.
Enable Auto-Shutdown:	Auto-Shutdown forces the termination of modules that have lost communication with their respective physical device. This capability is needed for plug-and-play support. By default, Auto-Shutdown is enabled. If automatic termination of modules when they have lost communication is not desired, this selection should be disabled.
Enable Subnet Match:	This selection allows you to specify whether or not IP devices should only be detected/ discovered if they are on the same IP Subnet as the Master.
Purge Bound Modules on Reset:	This selection indicates that all modules should be deleted from the bound directory upon the next reboot. During the binding process, the associated Duet modules for a device are copied from the /unbound directory into a protected /bound area. Due to the dynamic nature of Java class loading, it is not safe to delete a running .JAR file. Therefore, this selection provides the administrator the capability of removing existing modules upon reboot by forcing a re-acquisition of the module at bind time. This selection is a one-time occurrence - upon the next reboot, the selection is cleared.
Enable/Disable Module Search via Internet:	This option toggles the capability of searching the Internet (either AMX's site or a device specified site) for a device’s compatible Duet modules. This capability is automatically disabled if the Master does not have Internet connectivity. Upon enabling Internet connectivity, the AMX License Agreement is displayed. The License Agreement must be accepted for Internet Module search feature to be enabled. When this feature is enabled, the Master queries either AMX's Online database of device Modules and/or pulls Modules from a separate site specified by the manufacturer's device. You can later disable this feature by toggling this button.

2. Press the **Accept** button to save your changes.

Managing Device Modules

Use the **Manage Device Modules** set of options to archive or delete modules from the Master. All modules currently present on the Master are indicated in the Module list.

Archiving a Module

1. Select a module and click the **Archive Module** button.
2. This action copies the selected module (*.JAR) file to your PC.
3. The system will prompt you to specify a target directory to save the module file to.

Deleting a Module

Select a module and click the **Delete Module** button. This action deletes the selected module from the **/unbound** directory.

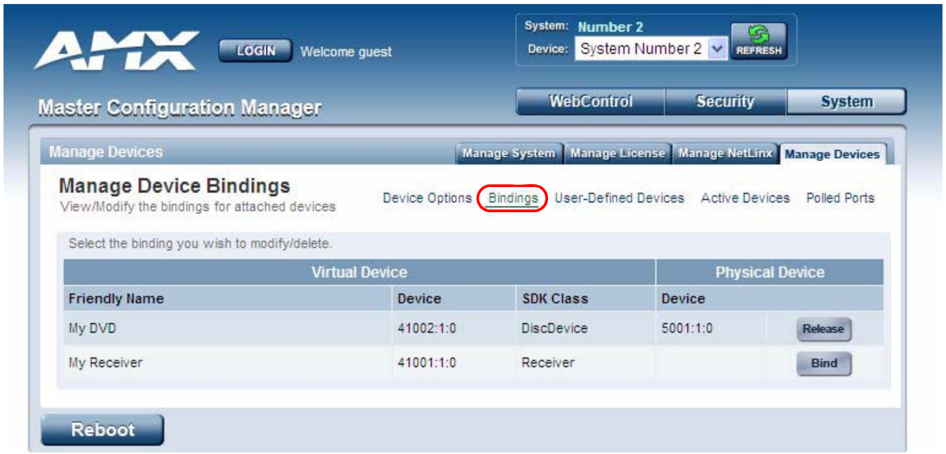
Note: *Any corresponding module within the /bound directory will not be deleted. Bound modules must be deleted via the Purge Bound Modules on Reset selection described within the Configure Device Bindings section.*

To browse for a Module file and then upload it to the Master:

1. Click the *Browse* button next to the **Select a module to upload** text field to browse for Duet Modules on your PC/ Network.
2. Select the JAR file that you want to upload to the Master.
3. Click the **Submit** button to upload a copy of the selected JAR file to the target Master's **/unbound** directory.
    - If a file of the same specified name already exists within the **/unbound** directory, the system will prompt you to confirm overwriting the existing file.
    - Only JAR file types are allowed for Upload to the target Master.

Manage Devices - Bindings

Click the **Bindings** link (in the *Manage Devices* tab) to access the **Manage Device Bindings** page (FIG. 61). Use the options on this page to configure application-defined Duet virtual devices with discovered physical devices.



Manage Device Bindings

View/Modify the bindings for attached devices

Select the binding you wish to modify/delete.

Virtual Device			Physical Device	
Friendly Name	Device	SDK Class	Device	
My DVD	41002:1:0	DiscDevice	5001:1:0	Release
My Receiver	41001:1:0	Receiver		Bind

FIG. 61 System - Manage Devices (Manage Device Bindings)

The table on this page displays a list of all application-defined devices, including each device’s "Friendly Name", the Duet virtual device’s D:P:S assignment, the associated Duet Device SDK class (indicating the type of the device), and the physical device’s D:P:S assignment. This information has to be pre-coded into the NetLinx file currently on the Master.

Configuring Application-Defined Devices

Elements such as `DUET_DEV_TYPE_DISC_DEVICE` and `DUET_DEV_POLLED` are defined within the NetLinx.axi file.

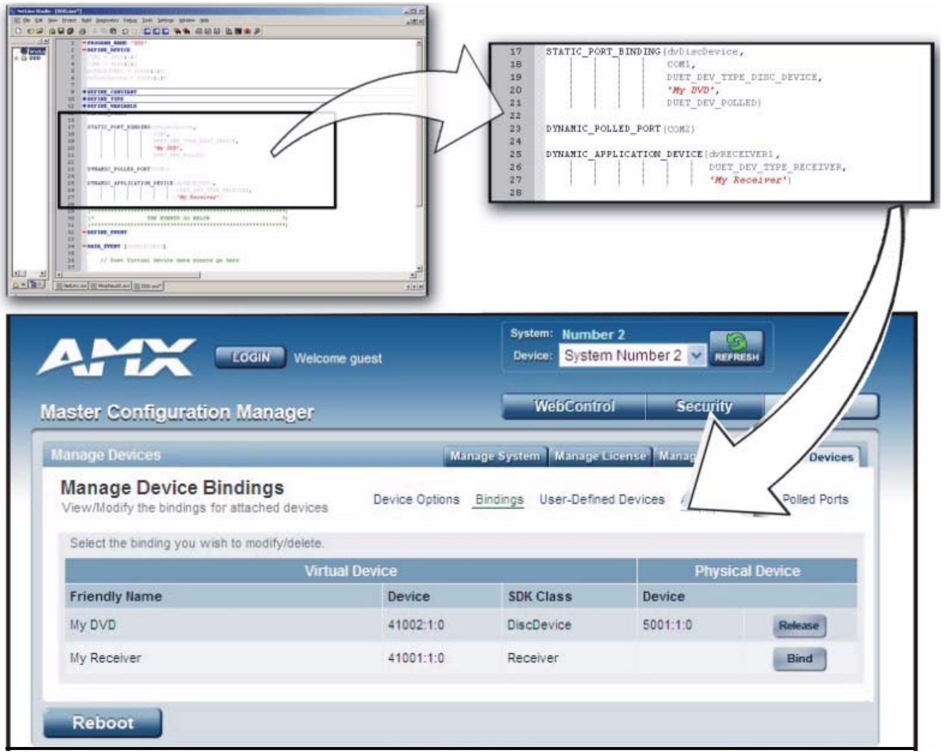
The NetLinx.axi file contains both the new API definitions, as well as the pre-defined constants that are used as some of the API arguments (ex: `DUET_DEV_TYPE_DISC_DEVICE`).

Note: *Physical device names are typically prefixed with "**dv**" and Virtual device names are typically prefixed with "**vdv**".*

Example Code:

```
PROGRAM_NAME='DDD'
DEFINE_DEVICE
COM1 = 5001:1:0
COM2 = 5001:2:0
dvRECEIVER1 = 41000:1:0
dvDiscDevice = 41001:1:0

DEFINE_CONSTANT
DEFINE_TYPE
DEFINE_VARIABLE
DEFINE_START


STATIC_PORT_BINDING(dvDiscDevice, COM1, DUET_DEV_TYPE_DISC_DEVICE,
    'My DVD', DUET_DEV_POLLED)


DYNAMIC_POLLED_PORT(COM2)

DYNAMIC_APPLICATION_DEVICE(dvRECEIVER1, DUET_DEV_TYPE_RECEIVER,
   'My Receiver')

(***********************************************************)
(*                THE EVENTS GO BELOW                      *)
(***********************************************************)
DEFINE_EVENT

DATA_EVENT [dvRECEIVER1]
{
    // Duet Virtual device data events go here
}
```

Sample code can be found within the DEFINE_START section, as shown in FIG. 62:



```
STATIC_PORT_BINDING(dvDiscDevice,
                    COM1,
                    DUET_DEV_TYPE_DISC_DEVICE,
                    'My DVD',
                    DUET_DEV_POLLED)

DYNAMIC_POLLED_PORT(COM2)

DYNAMIC_APPLICATION_DEVICE(dvRECEIVER1,
                           DUET_DEV_TYPE_RECEIVER,
                           'My Receiver')
```

Manage Device Bindings

View/Modify the bindings for attached devices

Select the binding you wish to modify/delete.

Virtual Device			Physical Device	
Friendly Name	Device	SDK Class	Device	
My DVD	41002:1:0	DiscDevice	5001:1:0	Release
My Receiver	41001:1:0	Receiver		Bind

FIG. 62 Manage Device Bindings page - showing the NetLinx code relation

This code gives the Master a “heads-up” notification to look for those devices meeting the criteria outlined within the code.

Application Devices and Association Status

There are two types of application devices: **Static Bound** application devices and **Dynamic** application devices:

- **Static Bound** application devices specify both a Duet virtual device and its associated Device SDK class type, as well as a NetLinx physical device port to which the application device is always associated (i.e. statically bound).
- **Dynamic** application devices specify both the Duet virtual device and its associated Device SDK with no association to a physical port. Binding of an application device to a physical device/port occurs at run-time (either via auto-binding or manual binding).

Application devices that have a "bound" physical device display their physical device ID within the **Physical Device** column. If an associated Duet module has been started to communicate with the device, its associated property information is displayed in a mouse-over popup dialog when the cursor hovers over the physical device ID (see FIG. 63 on page 62).

Each entry in the table has one of four buttons to the right of the Physical Device D:P:S assignment:

- **Static Bound** application devices will either be **blank,** or display a **Release** button:
  - Static Bound application devices that have not yet detected a physical device attached to their associated port have a **blank** button.
  - Once a physical device is detected and its associated Duet module has been started, a **Release** button is then displayed. Click **Release** to force the associated Duet module to be destroyed and the firmware then returns to detecting any physical devices attached to the port.
- **Dynamic** application devices either display a **Bind** or **Unbind** button:
  - Dynamic application devices that have been bound display an **Unbind** button. When the user selects **Unbind**, any associated Duet module is then destroyed and the "link" between the application device and the physical device is then broken.
  - Dynamic application devices that have not been bound to a physical device display a **Bind** button. When this button is selected, a secondary display appears with a listing of all available unbound physical devices that match the application device's Device SDK class type.

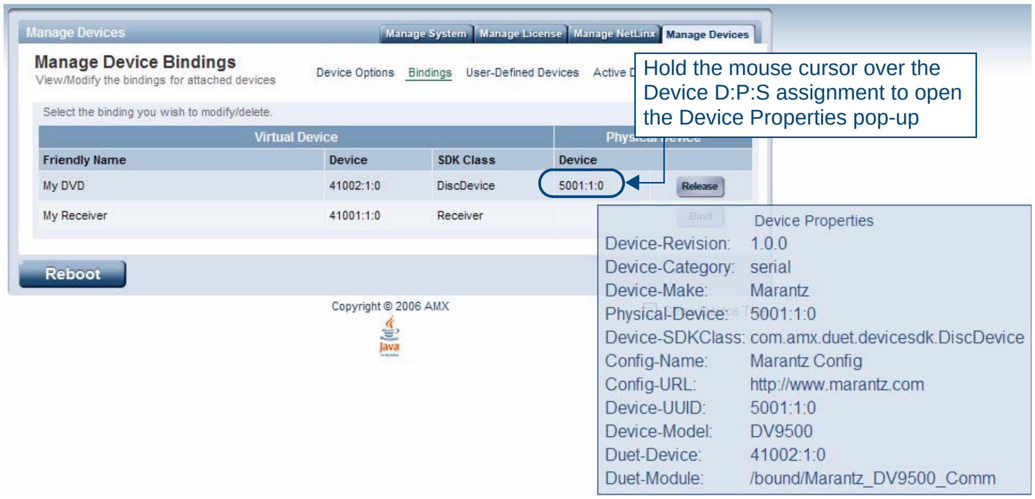
Note: *If a currently bound device needs to be replaced or a Duet Module needs to be swapped out, the device should be unbound and the new module/driver should then be bound.*

The administrator/user can then select one of the available physical devices to bind with the associated application device. When the **Save** button is selected, the binding is created and a process begins within the target Master to find the appropriate Duet Module driver. Once a driver is found, the Duet Module is then started and associated with the specified application device (Duet virtual device). If the **Cancel** button is selected, the binding activity is then aborted.

Note: *If the manufacturer device does not support Dynamic Device Discovery (DDD) beaconing, you must use the Add New Device page to both create and manage those values necessary to add a dynamic physical device. This process is described in detail within the following section.*

Viewing Physical Device Properties

Hold the mouse cursor over the Physical Device - **Device** entry in the table to display detailed device properties for that device, in a pop-up window (FIG. 63).



Manage Device Bindings
View/Modify the bindings for attached devices

Select the binding you wish to modify/delete.

Virtual Device			Physical Device	
Friendly Name	Device	SDK Class	Device	
My DVD	41002:1:0	DiscDevice	5001:1:0	Release
My Receiver	41001:1:0	Receiver		

Hold the mouse cursor over the Device D:P:S assignment to open the Device Properties pop-up

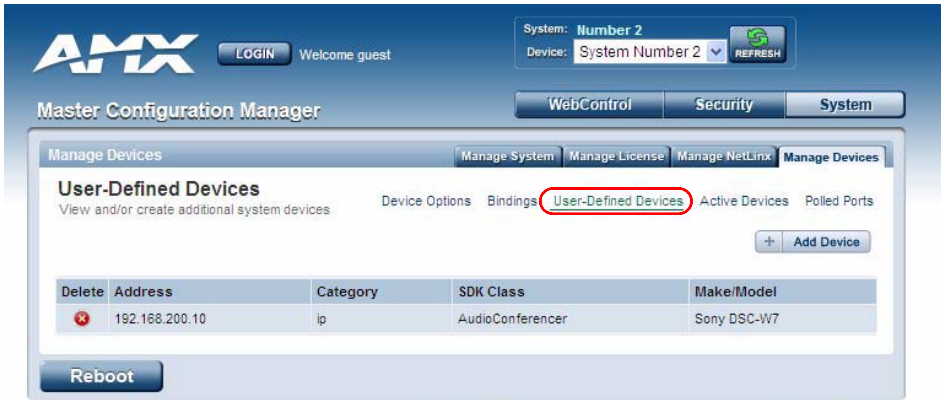
Device Properties

Device-Revision:	1.0.0
Device-Category:	serial
Device-Make:	Marantz
Physical-Device:	5001:1:0
Device-SDKClass:	com.amx.duet.devicesdk.DiscDevice
Config-Name:	Marantz Config
Config-URL:	http://www.marantz.com
Device-UUID:	5001:1:0
Device-Model:	DV9500
Duet-Device:	41002:1:0
Duet-Module:	/bound/Marantz_DV9500_Comm

FIG. 63 Manage Device Bindings - Device Properties pop-up

Manage Devices - User-Defined Devices

Click the **User-Defined Devices** link (in the *Manage Devices* tab) to access the **User-Defined Devices** page (FIG. 64). This page provides a listing with all of the dynamic devices that have been discovered in the system, and allows you to add and delete User-Defined Devices.



System: Number 2
Device: System Number 2

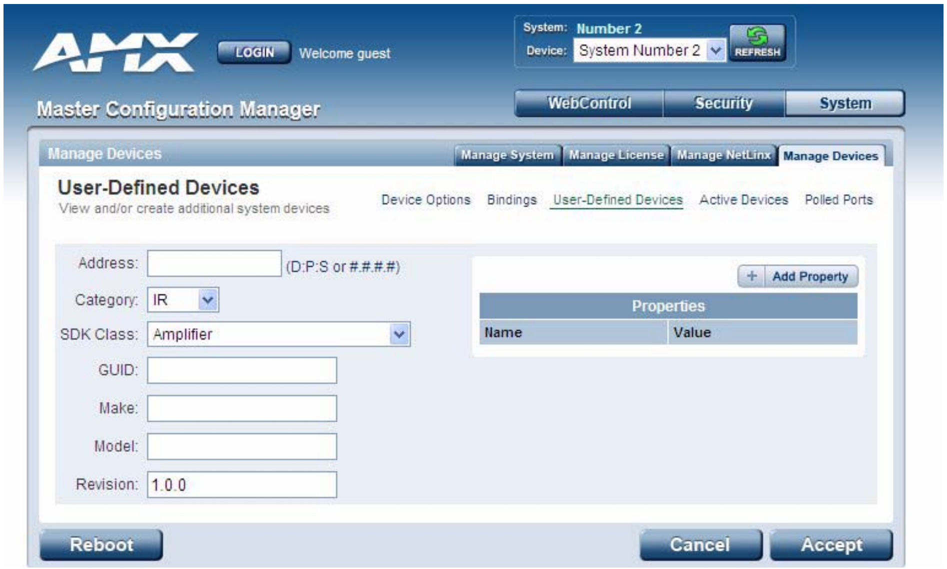
User-Defined Devices
View and/or create additional system devices

Delete	Address	Category	SDK Class	Make/Model
☒	192.168.200.10	ip	AudioConferencer	Sony DSC-W7

FIG. 64 System - Manage Devices (User-Defined Devices)

Adding a User-Defined Device

1. Click the **Add Device** button (in the User-Defined Devices page) to access the **Add User Defined Device** page (FIG. 65):



User-Defined Devices
View and/or create additional system devices

Address: (D:P:S or #.#.#.#)
Category: IR
SDK Class: Amplifier
GUID:
Make:
Model:
Revision: 1.0.0

FIG. 65 User-Defined Devices - Add User Defined Device

2. Fill in the device information fields, as described in the following tables:

User-Defined Device Information Fields	
Address:	Enter the address of the physical device in the Address field. This information can be either the NetLinx Master port value (D:P:S) or an IP Address (#.#.#.#).
Category:	Use the drop-down list to select the control method associated with the physical target device (*IR*, *IP*, *Serial*, *Relay*, *Other*).
SDK Class:	Use the drop-down list to select the closest Device SDK class type match for the physical target device. The **SDK-Class Types** table (below) provides a listing of the available choices.
GUID:	Enter the manufacturer-specified device's GUID (Global Unique Identification) information. Either the GUID or Make/Model must be specified in this field.
Make:	Enter the name of the manufacturer for the device being used (ex: Sony, ONKYO, etc.) • Up to 55 alpha-numeric characters • Either the GUID or Make/Model must be specified within this field. • Spaces in the name will be converted to underscores.
Model:	Enter the model number of the device being used (ex: Mega-Tuner 1000) • Up to 255 alpha-numeric characters • Either the GUID or Make/Model must be specified within this field.
Revision	Enter the firmware version used by the target device. • Text is required within this field. • The version must be in the format: major.minor.micro (where major, minor, and micro are numbers). An example is: 1.0.0 (revision 1.0.0 of the device firmware).

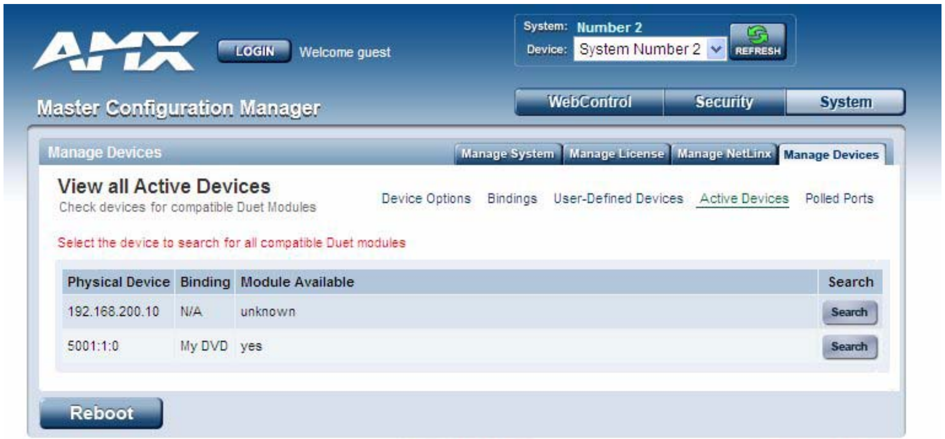
SDK-Class Types			
Amplifier	Digital Video Recorder	PreAmpSurroundSoundProcessor	Utility
AudioConferencer	Disc Device	Receiver	VCR
AudioMixer	DocumentCamera	RelayDevice	VideoConferencer
AudioProcessor	HVAC	Security System	VideoProcessor
AudioTape	IODevice	Sensor Device	VideoProjector
AudioTunerDevice	Keypad	SettopBox	VideoWall
Camera	Light	SlideProjector	VolumeController
Digital Media Decoder	Monitor	Switcher	Weather
Digital Media Encoder	Motor	Text Keypad	
Digital Media Server	MultiWindow	TV	
Digital Satellite System	PoolSpa	UPS	

3. Once you are done creating the profile for the new device, click the **Add Property** button to access the **Name** and **Value** fields property information for association with the new User Defined Device.

4. Click the **Accept** button. The new device is indicated in the list of discovered physical devices (in the *User-Defined Devices* page).

Manage Devices - Active Devices

Click the **Active Devices** link (in the *Manage Devices* tab) to access the **View All Active Devices** page (FIG. 66). The options on this page allow you to check devices for compatible Duet Modules.



System: Number 2

Device: System Number 2

View all Active Devices

Check devices for compatible Duet Modules

Select the device to search for all compatible Duet modules

Physical Device	Binding	Module Available	Search
192.168.200.10	N/A	unknown	Search
5001:1:0	My DVD	yes	Search

FIG. 66 System - Manage Devices (Active Devices)

Searching For All Compatible Duet Modules for a Selected Device

1. Click the Search button for the device that you want to find a Duet Module for. This action initiates a search for compatible modules, based on the following options:

   - Unless the **Disable Module Search via the Internet** option was selected in the Manage Devices page (*see the Manage Devices - Device Options* section on page 58*)*, the search includes a query of the AMX online database as well as any manufacturer specified URLs that match the IP Address of the physical device for a compatible module.
   - If the device specified a **URL** in its DDD beacon, the file is retrieved from the URL either over the Internet or from the physical device itself, provided the device has an inboard HTTP or FTP server.
   - If **Module Search via Internet** is ***NOT enabled***, the search does NOT query the AMX online database nor will it pull any manufacturer specified URLs that do not match the IP Address of the physical device itself.

   Modules that are retrieved from either the Internet or from the manufacturer's device are then placed into the **/ unbound** directory and automatically overwrite any existing module of the same name.

2. Once a list of all compatible modules is compiled, the Available Modules list is displayed on this page.

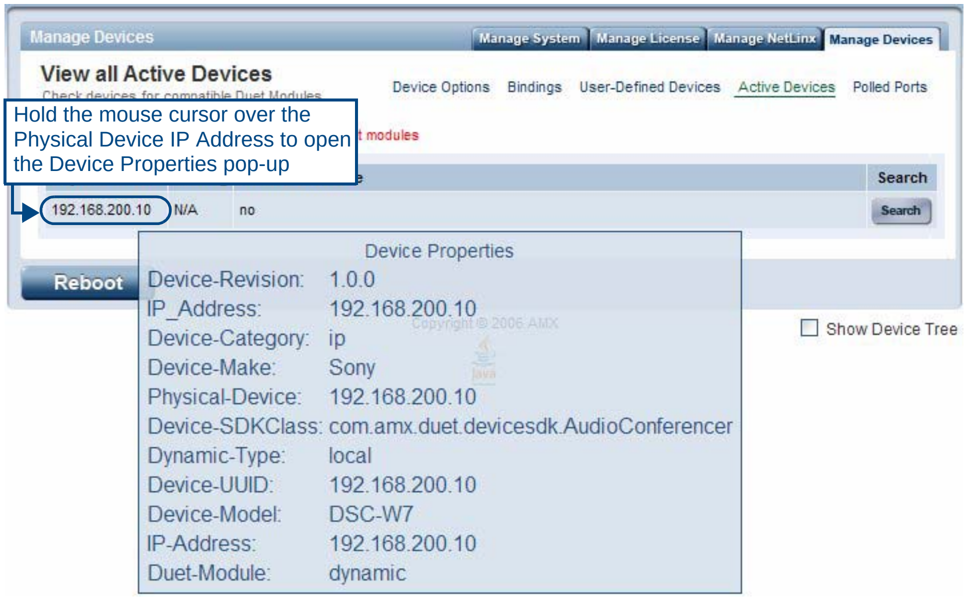
   Each module is listed with its calculated “match” value. The greater the “match” value, the better the match between the Duet Module's properties and the physical device's properties.

3. Select a module and click the **Accept** button to associate the selected Duet module with the physical device.

***Note:** This action will not affect any currently running Duet module associated with the physical device. The module is associated with the device upon reboot.*

Viewing Physical Device Properties

Hold the mouse cursor over the **Device** entry in the table to display detailed device properties for that device, in a pop-up window (FIG. 67).



Hold the mouse cursor over the Physical Device IP Address to open the Device Properties pop-up

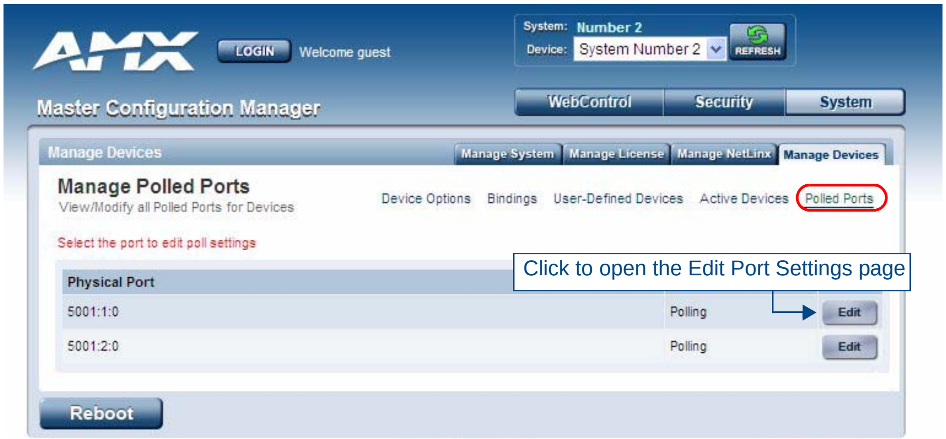
Device Properties

Device-Revision: 1.0.0
IP_Address: 192.168.200.10
Device-Category: ip
Device-Make: Sony
Physical-Device: 192.168.200.10
Device-SDKClass: com.amx.duet.devicesdk.AudioConferencer
Dynamic-Type: local
Device-UUID: 192.168.200.10
Device-Model: DSC-W7
IP-Address: 192.168.200.10
Duet-Module: dynamic

FIG. 67 View All Active Devices - Device Properties pop-up

Manage Devices - Manage Polled Ports

Click the **Polled Ports** link (in the *Manage Devices* tab) to access the **Manage Polled Ports** page (FIG. 68). The options on this page allow you to view/modify settings for all polled ports in the System.



Manage Polled Ports

View/Modify all Polled Ports for Devices

Select the port to edit poll settings

Physical Port		
5001:1:0	Polling	Edit
5001:2:0	Polling	Edit

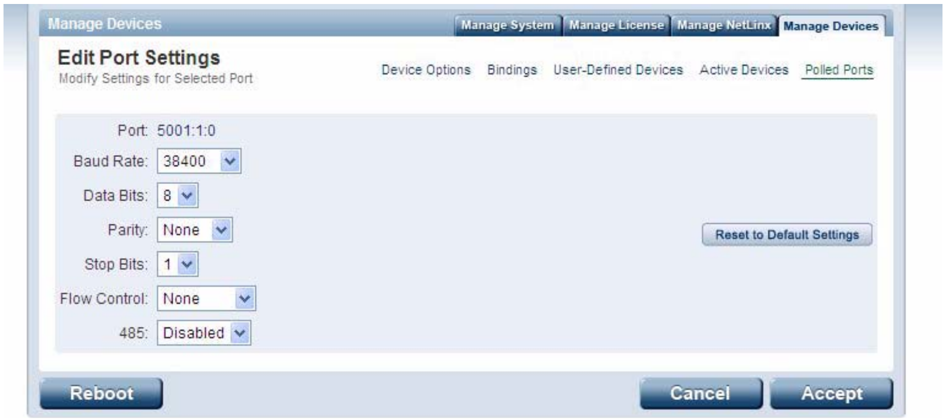
Click to open the Edit Port Settings page

FIG. 68 System - Manage Devices (Manage Polled Ports)

Note: *Polled Ports must be specified in the Master's code in order for this page to be populated.*

Editing Polled Port Settings

Click the **Edit** button for a port in the Physical Port list to access the *Edit Port Settings* page (FIG. 69):



Edit Port Settings

Modify Settings for Selected Port

Port: 5001:1:0

Baud Rate: 38400

Data Bits: 8

Parity: None

Stop Bits: 1

Flow Control: None

485: Disabled

FIG. 69 Manage Polled Ports - Edit Port Settings

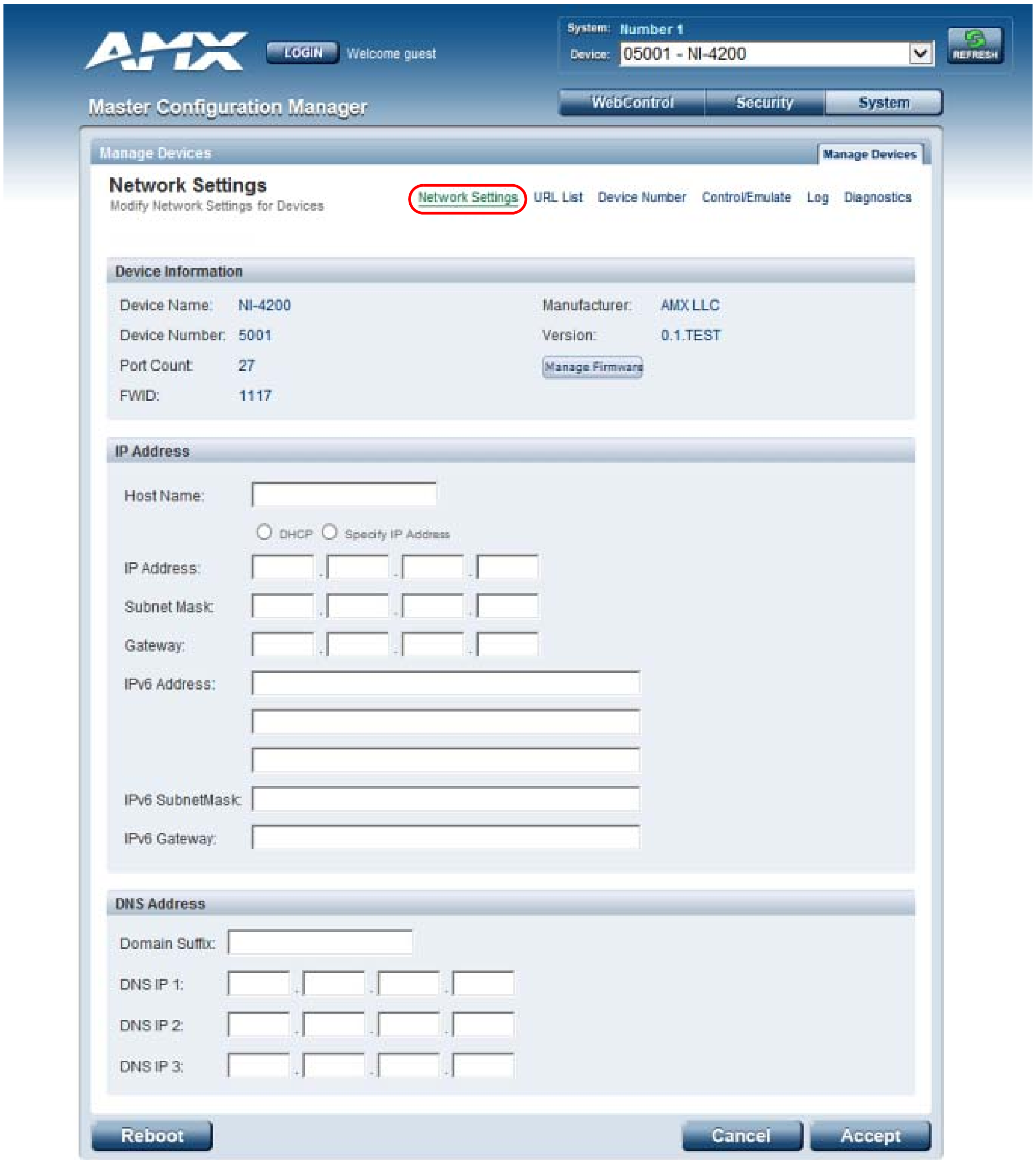
Use the drop-down menus to modify the Port settings.

Click **Reset to Default Settings** to return this port to its default configuration:

Default Port Settings	
Baud Rate:	9600
Data Bits:	8
Parity:	None
Stop Bits:	1
Flow Control:	None
485:	Disabled

Manage Devices - Network Settings

With the Master selected in the *Device* drop-down menu, click the **Network Settings** link (in the *Manage Devices* tab) to access the **Network Settings** page (FIG. 70). Use the options on this page to view/edit the Master’s network settings.



System: Number 1

Device: 05001 - NI-4200

Network Settings

Modify Network Settings for Devices

Device Information

Device Name:	NI-4200	Manufacturer:	AMX LLC
Device Number:	5001	Version:	0.1.TEST
Port Count:	27		
FWID:	1117		

IP Address

Host Name:

○ DHCP ○ Specify IP Address

IP Address: . . .

Subnet Mask: . . .

Gateway: . . .

IPv6 Address:

IPv6 SubnetMask:

IPv6 Gateway:

DNS Address

Domain Suffix:

DNS IP 1: . . .

DNS IP 2: . . .

DNS IP 3: . . .

FIG. 70 System - Manage Devices (Network Settings)

Manage Devices - URL List

With the Master selected in the *Device* drop-down menu, click the **URL List** link (in the *Manage Devices* tab) to access the **URL List** page (FIG. 71). The options on this page allow you to view and edit the URL List of devices for the Master.

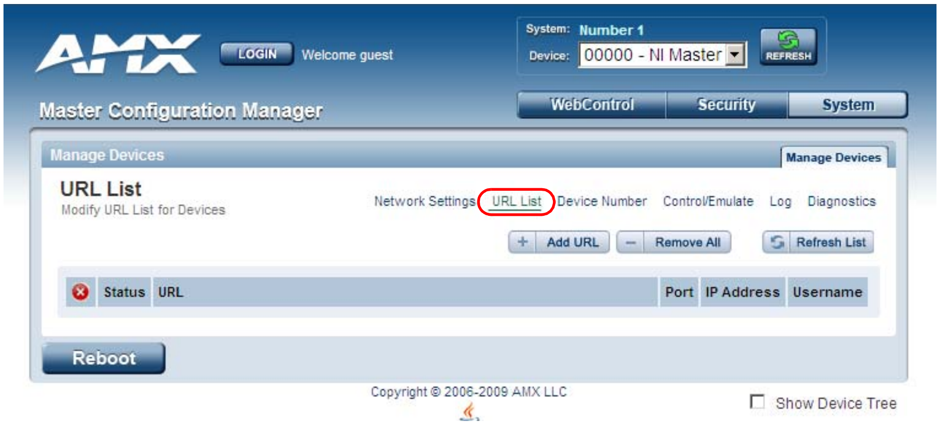
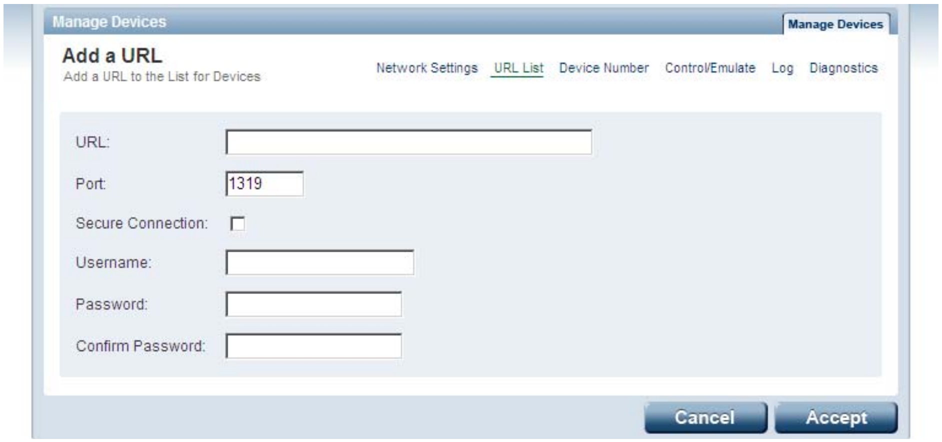


FIG. 71 System - Manage Devices (URL List)

Adding a URL to the Master's List of Devices

In the *Manage Devices - URL List* page, click the **Add URL** button to open the *Add a URL* page (FIG. 72):



URL:

Port: 1319

Secure Connection: □

Username:

Password:

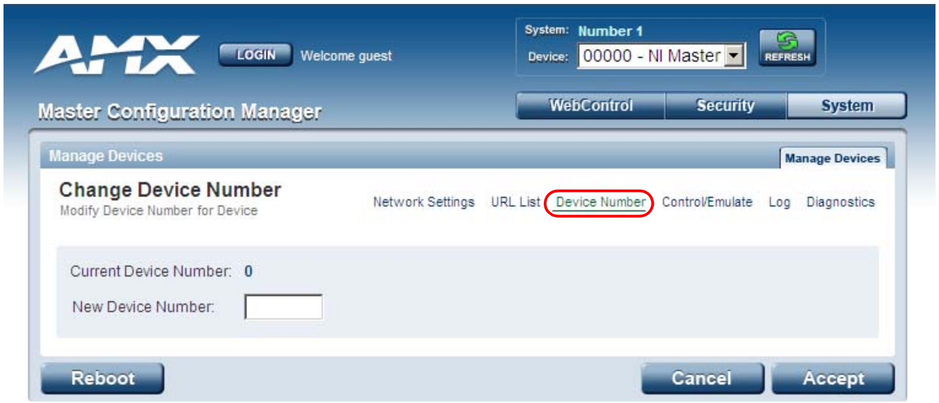
Confirm Password:

FIG. 72 Add a URL page

Fill in the fields and click **Accept** to save the changes and add this information to the URL List.

Manage Devices - Device Number

With the Master selected in the *Device* drop-down menu, click the **Device Number** link (in the *Manage Devices* tab) to access the **Change Device Number** page (FIG. 73). The options on this page allow you to change the device number on the Master.



System: Number 1

Device: 00000 - NI Master

Change Device Number

Modify Device Number for Device

Current Device Number: 0

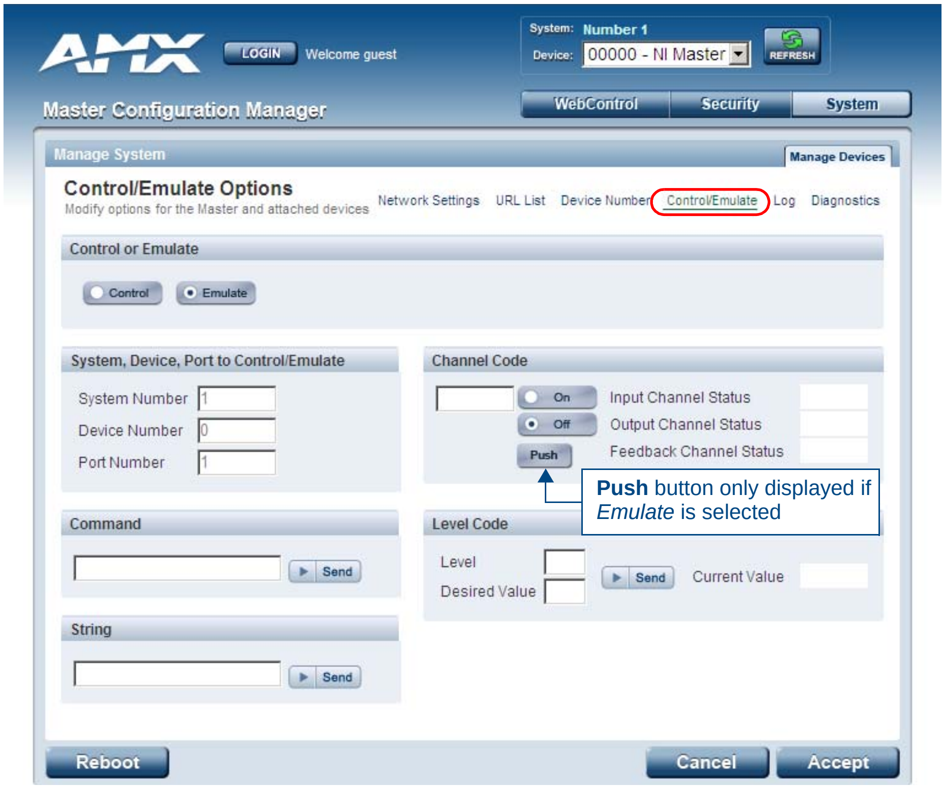
New Device Number:

FIG. 73 System - Manage Devices (Device Number)

- Default = 0 (zero)
- Note that in most cases, the Device Number for Masters should remain set to zero.

Manage Devices - Control/Emulate

With the Master selected in the *Device* drop-down menu, click the **Control/Emulate** link (in the *Manage Devices* tab) to access the **Control/Emulate Options** page (FIG. 74).



System: Number 1

Device: 00000 - NI Master

Control/Emulate Options

Modify options for the Master and attached devices

Control or Emulate: ○ Control ● Emulate

System, Device, Port to Control/Emulate

System Number: 1

Device Number: 0

Port Number: 1

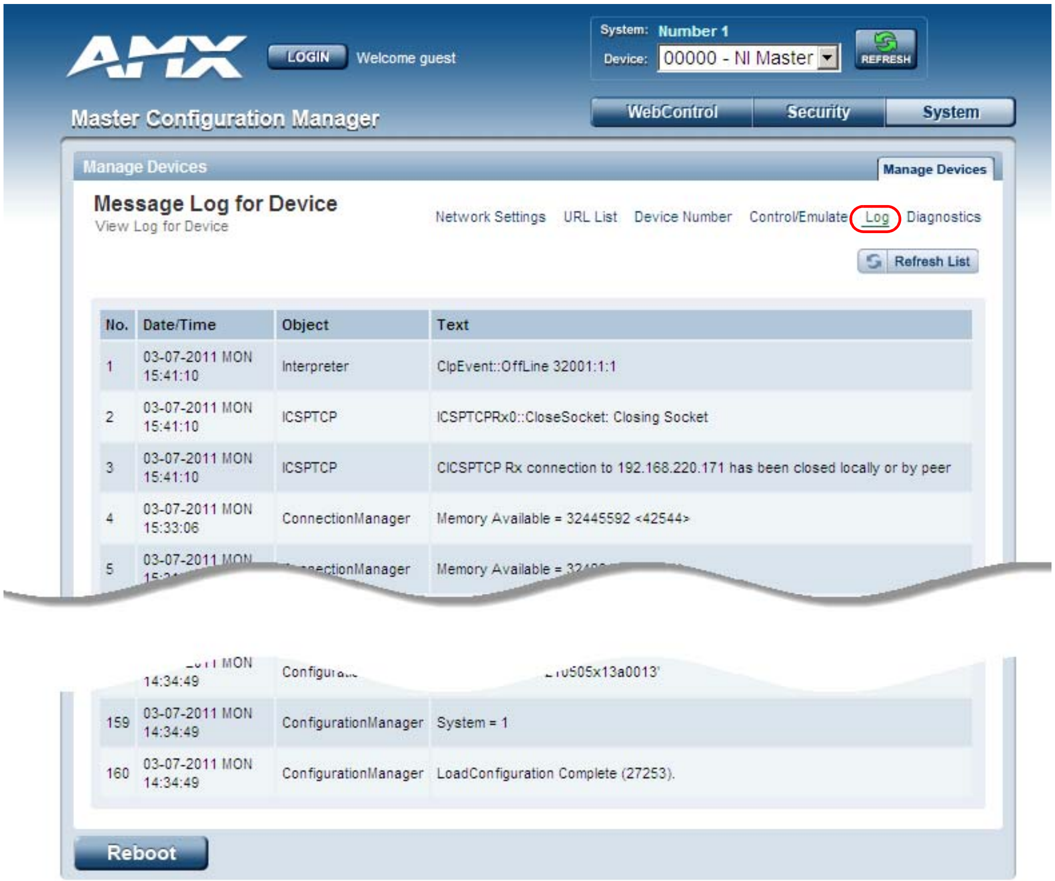
Push button only displayed if *Emulate* is selected

FIG. 74 Manage System (Control/Emulate Options)

This page can also be accessed via the *Manage System* options, as described in the *Manage System - Control/Emulate Options* section on page 36. See the *Controlling or Emulating a System Device* section on page 37 for details.

Manage Devices - Log

With the Master selected in the *Device* drop-down menu, click the **Log** link (in the *Manage Devices* tab) to access the **Message Log For Device** page (FIG. 75). This page displays message logs for the Master.



Message Log for Device

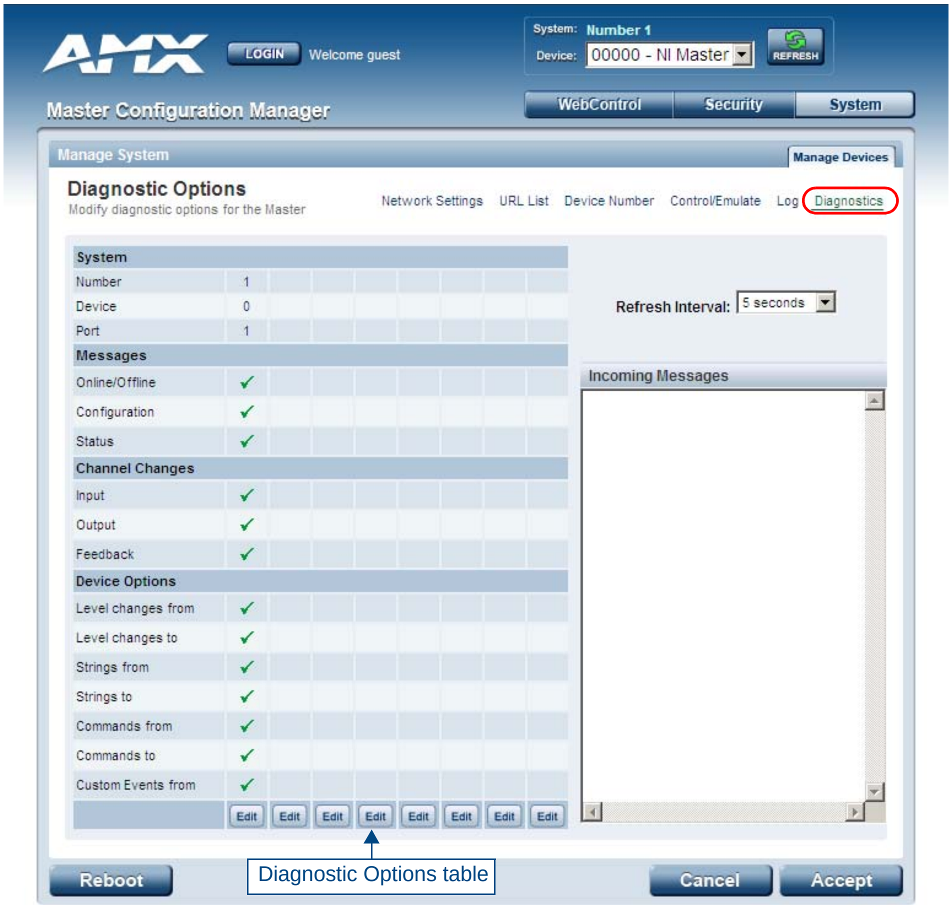
View Log for Device

No.	Date/Time	Object	Text
1	03-07-2011 MON 15:41:10	Interpreter	ClpEvent::OffLine 32001:1:1
2	03-07-2011 MON 15:41:10	ICSPTCP	ICSPTCPRx0::CloseSocket: Closing Socket
3	03-07-2011 MON 15:41:10	ICSPTCP	CICSPTCP Rx connection to 192.168.220.171 has been closed locally or by peer
4	03-07-2011 MON 15:33:06	ConnectionManager	Memory Available = 32445592 <42544>
5	03-07-2011 MON 15:3	nectionManager	Memory Available = 324
	11 MON 14:34:49	Configura	10505x13a0013'
159	03-07-2011 MON 14:34:49	ConfigurationManager	System = 1
160	03-07-2011 MON 14:34:49	ConfigurationManager	LoadConfiguration Complete (27253).

FIG. 75 Manage System (Message Log For Device)

Manage Devices - Diagnostics

With the Master selected in the *Device* drop-down menu, click the **Diagnostics** link (in the *Manage Devices* tab) to access the **Diagnostics Options** page (FIG. 76).



Diagnostic Options

Modify diagnostic options for the Master

System								
Number	1							
Device	0							
Port	1							
Messages								
Online/Offline	✓							
Configuration	✓							
Status	✓							
Channel Changes								
Input	✓							
Output	✓							
Feedback	✓							
Device Options								
Level changes from	✓							
Level changes to	✓							
Strings from	✓							
Strings to	✓							
Commands from	✓							
Commands to	✓							
Custom Events from	✓							
	Edit	Edit	Edit	Edit	Edit	Edit	Edit	Edit

Refresh Interval: 5 seconds

Incoming Messages

FIG. 76 Diagnostics Options Page (with diagnostic messages enabled)

This page can also be accessed via the *Manage System* options, as described in the *Manage System - Diagnostics Options* section on page 39.

See the *Enabling Diagnostics on a Selected System Device* section on page 40 for details.

NetLinx Programming

Overview

This section describes the Send_Commands, Send_Strings, and Channel commands you can use to program the Master. The examples in this section require a declaration in the DEFINE_DEVICE section of your program to work correctly.

Refer to the *NetLinx Programming Language* instruction manual for specifics about declarations and DEFINE_DEVICE information.

***Note:** All file names on the X-Series controllers are case sensitive. This includes all user files created or used within NetLinx or Java code. If you have legacy code that uses files, it is important that you verify that every reference to each file is consistent with regard to case. If your legacy code generates an error when accessing a file, it is likely due to inconsistent use of case in the filename.*

Port Assignments by NetLinx Master

Port Assignments By Master

Master	RS-232	RS-232/422/485	IR/Serial	IR/RX	Relays	I/O	PoE
NX-1200	Port 2	Port 1	Ports 11-12	Port 20	N/A	Port 22	N/A
NX-2200	Ports 2-4	Port 1	Ports 11-14	N/A	Port 21	Port 22	N/A
NX-3200	Ports 2-4, 6-8	Ports 1, 5	Ports 11-18	N/A	Port 21	Port 22	N/A
NX-4200	Ports 2-4, 6-8	Ports 1, 5	Ports 11-18	N/A	Port 21	Port 22	Ports 24-27

Master SEND_COMMANDs

These commands are specific to the Master and not the Controller. These commands are sent to the DPS 0:1:0 (the Master you are connected to).

A device (<DEV>) must first be defined in the NetLinx programming language with values for the Device: Port: System (<D:P:S>).

Master SEND_COMMANDs

Command	Description

CLOCK	Set the date and time on the Master. The date and time settings are propagated over the local bus.
	Syntax:
	`SEND_COMMAND <DEV>,"'CLOCK <mm-dd-yyyy> <hh:mm:ss>'"`
	Variables:
	mm-dd-yyyy = Month, day, and year. Month and day have 2 significant digits. Year has 4 significant digits.
	hh-mm-ss = Hour, minute, and seconds. Each using only 2 significant digits.
	Example:
	`SEND_COMMAND 0,"'CLOCK 04-12-2005 09:45:31'"`
	Sets the Master's date to April 12, 2005 with a time of 9:45 am.

Master SEND_COMMANDs (Cont.)	
Command	Description

G4WC	Add G4 Web Control devices to Web control list displayed by the Web server in a browser. The internal G4WC Send command (to Master 0:1:0) has been revised to add G4 Web Control devices to Web control list displayed in the browser.
	Syntax:
	`SEND_COMMAND <D:P:S>,"'G4WC "Name/Description",IP Address/URL,IP Port,Enabled'"`
	Variables:
	• Name/Description = A string, enclosed in double quotes, that is the description of the G4 Web Control instance. It is displayed in the browser.
	• IP Address/URL = A string containing the IP Address of the G4 Web Control server, or a URL to the G4 Web Control server.
	• IP Port = A string containing the IP Port of the G4 Web Control Server.
	• Enabled = 1 or 0. If it is a 1 then the link is displayed. If it is a 0 then the link is disabled.
	The combination of Name/Description, IP Address/URL, and IP Port are used to determine each unique listing.
	Example:
	`SEND_COMMAND 0:1:0,"'G4WC "Bedroom",192.168.1.2,5900,1'"`
	Adds the BEDROOM control device using the IP Address of 192.168.1.2.

~IGNOREEXTERNALCLOCKCOMMANDS	Set the Master so that it cannot have it's time set by another device which generates a 'CLOCK' command.
	Syntax:
	`SEND_COMMAND <D:P:S>,"'~IGNOREEXTERNALCLOCKCOMMANDS'"`
	Example:
	`SEND_COMMAND 0:1:0,"'~IGNOREEXTERNALCLOCKCOMMANDS'"`

Master IP Local Port SEND_COMMANDs

These commands are specific to the Master and not the Controller. These commands are sent to the DPS 0:1:0 (the Master). A device must first be defined in the NetLinx programming language with values for the Device: Port: System.

In these programming examples, <DEV> = Device. The term <D:P:S> = Device:Port:System.

Master IP Local Port SEND_COMMANDs	
Command	Description

UDPSENDTO	Set the IP and port number of the UDP local ports destination for sending future packets. This is only available for Type 2 and Type 3 Local Ports. Type 2 and Type 3 are referring to the protocol type that is part of the IP_CLIENT_OPEN call (4th parameter).
	Type 1 is TCP.
	Type 2 is UDP (standard)
	Type 3 is UDP (2 way)
	The NetLinx.axi defines constants for the protocol types:
	CHAR IP_TCP = 1
	CHAR IP_UDP = 2
	CHAR IP_UDP_2WAY = 3
	Syntax:
	`SEND_COMMAND <D:P:S>,"'UDPSENDTO-<IP or URL>:<UDP Port Number>'"`
	Variables:
	• IP or URL = A string containing the IP Address or URL of the desired destination.
	• UDP Port Number = A String containing the UDP port number of the desired destination.
	Example 1:
	`SEND_COMMAND 0:3:0,"'UDPSENDTO-192.168.0.1:10000'"`
	Any subsequent SEND_STRING to 0:3:0 are sent to the IP Address 192.168.0.1 port 10000.
	Example 2:
	`SEND_COMMAND 0:3:0,"'UDPSENDTO-myUrl.com:15000'"`
	Any subsequent SEND_STRING to 0:3:0 are sent to the URL myURL.com port 15000.

LED SEND_COMMANDs

Note: *The following sections only apply to the integrated controller component of the NX-series controllers.*

The following commands enable or disable the LEDs on the Controller.

In the examples: <DEV> = Port 1 of the device. Sending to port 1 of the controller affects all ports.

LED SEND_COMMANDs	
Command	Description

LED-DIS	Disable all LEDs (on 32 LED hardware) for a port. Regardless of whether or not the port is active, the LED will not be lit.
	Issue this command to port 1 to disable all the LEDs on the Controller.
	When activity occurs on a port(s) or Controller, the LEDs will not illuminate.
	Syntax:
	`SEND_COMMAND <DEV>,"'LED-DIS'"`
	Example:
	`SEND_COMMAND Port_1,"'LED-DIS'"`
	Disables all the LEDs on Port 1 of the Controller.

LED-EN	Enable the LED (on 32 LED hardware) for a port. When the port is active, the LED is lit. When the port is not active, the LED is not lit.
	Issue the command to port 1 to enable the LEDs on the Controller (default setting). When activity occurs on a port(s) or Controller, the LEDs illuminate.
	Syntax:
	`SEND_COMMAND <DEV>,'LED-EN'`
	Example:
	`SEND_COMMAND System_1,'LED-EN'`
	Enables the System_1 Controller's LEDs.

RS232/422/485 Ports Channels

RS-232/422/485 Port Assignments By Master		
Master	RS-232	RS-232/422/485
NX-1200	Port 2	Port 1
NX-2200	Ports 2-4	Port 1
NX-3200	Ports 2-4, 6-8	Ports 1, 5
NX-4200	Ports 2-4, 6-8	Ports 1, 5

RS232/422/485 Ports Channels	
255 - CTS push channel	Reflects the state of the CTS input if a 'CTSPSH' command was sent to the port.

RS-232/422/485 SEND_COMMANDs

RS-232/422/485 SEND_COMMANDs	
Command	Description

B9MOFF	Disables 9-bit in 232/422/455 mode. By default, this returns the communication settings on the serial port to the last programmed parameters. This command works in conjunction with the 'B9MON' command.
	Syntax:
	`SEND_COMMAND <DEV>,"'B9MOFF'"`
	Example:
	`SEND_COMMAND RS232_1,"'B9MOFF'"`
	Sets the RS-232 port settings to match the port's configuration settings.

RS-232/422/485 SEND_COMMANDs (Cont.)

Command	Description

B9MON	Override and set the current communication settings and parameters on the RS-232 serial port to 9 data bits with one stop bit. This command works in conjunction with the 'B9MOFF' command.
	Syntax:
	`SEND_COMMAND <DEV>,"'B9MON'"`
	Example:
	`SEND_COMMAND RS232_1,"'B9MON'"`
	Resets the RS-232 port's communication parameters to nine data bits, one stop bit, and locks-in the baud rate.

CHARD	Set the delay time between all transmitted characters to the value specified (in 100 Microsecond increments).
	Syntax:
	`SEND_COMMAND <DEV>,"'CHARD-<time>'"`
	Variable:
	time = 0 - 255. Measured in 100 microsecond increments.
	Example:
	`SEND_COMMAND RS232_1,"'CHARD-10'"`
	Sets a 1-millisecond delay between all transmitted characters.

CHARDM	Set the delay time between all transmitted characters to the value specified (in 1-Millisecond increments).
	Syntax:
	`SEND_COMMAND <DEV>,"'CHARDM-<time>'"`
	Variable:
	time = 0 - 255. Measured in 1 millisecond increments.
	Example:
	`SEND_COMMAND RS232_1,"'CHARDM-10'"`
	Sets a 10-millisecond delay between all transmitted characters.

CLEAR FAULT	Forces a reset back to normal status.
	Syntax:
	`SEND_COMMAND <DEV>, "’CLEAR FAULT’"`
	Example:
	`SEND_COMMAND RS232_1,"’CLEAR FAULT’"`

CTSPSH	Enable Pushes, Releases, and Status information to be reported via channel 255 using the CTS hardware handshake input. This command turns On (enables) channel tracking of the handshaking pins.
	If Clear To Send (CTS) is set high, then channel 255 is On.
	Syntax:
	`SEND_COMMAND <DEV>,"'CTSPSH'"`
	Example:
	`SEND_COMMAND RS232_1,"'CTSPSH'"`
	Sets the RS232_1 port to detect changes on the CTS input.

CTSPSH OFF	Disable Pushes, Releases, and Status information to be reported via channel 255. This command disables tracking. Turns CTSPSH Off.
	Syntax:
	`SEND_COMMAND <DEV>,"'CTSPSH OFF'"`
	Example:
	`SEND_COMMAND RS232_1,"'CTSPSH OFF'"`
	Turns off CTSPSH for the specified device.

RS-232/422/485 SEND_COMMANDs (Cont.)

Command	Description
GET BAUD	Get the RS-232/422/485 port’s current communication parameters. The port sends the parameters to the device that requested the information. The port responds with: <port #>,<baud>,<parity>,<data>,<stop> [422] or [485] <ENABLED | DISABLED> Syntax: SEND_COMMAND <DEV>,"'GET BAUD'" Example: SEND_COMMAND RS232_1,"'GET BAUD'" System response example: Device 1,38400,N,8,1 422/485 DISABLED
GET FAULT	Check the activation status of fault detection on the port. Syntax: SEND_COMMAND <DEV>, "’GET FAULT’" Example: SEND_COMMAND RS232_1,"’GET FAULT’" Responds with DISABLED, NONE, or NO DEVICE.
GET STATUS	Check the fault detection status of the port. Syntax: SEND_COMMAND <DEV>, "’GET STATUS’" Example: SEND_COMMAND RS232_1,"’GET STATUS’" Responds with STATUS: NORMAL or STATUS: FAULT.
HSOFF	Disable hardware handshaking (default). Syntax: SEND_COMMAND <DEV>,"'HSOFF'" Example: SEND_COMMAND RS232_1,"'HSOFF'" Disables hardware handshaking on the RS232_1 device.
HSON	Enable RTS (ready-to-send) and CTS (clear-to-send) hardware handshaking. Syntax: SEND_COMMAND <DEV>,"'HSON'" Example: SEND_COMMAND RS232_1,"'HSON'" Enables hardware handshaking on the RS232_1 device.
RXCLR	Clear all characters in the receive buffer waiting to be sent to the Master. Syntax: SEND_COMMAND <DEV>,"'RXCLR'" Example: SEND_COMMAND RS232_1,"'RXCLR'" Clears all characters in the RS232_1 device's receive buffer waiting to be sent to the Master.
RXOFF	Disable the transmission of incoming received characters to the Master. Syntax: SEND_COMMAND <DEV>,"'RXOFF'" Example: SEND_COMMAND RS232_1,"'RXOFF'" Stops the RS232_1 device from transmitting received characters to the Master.

RS-232/422/485 SEND_COMMANDs (Cont.)

Command	Description

RXON	Start transmitting received characters to the Master (default).
	Enables sending incoming received characters to the Master.
	This command is automatically sent by the Master when a 'CREATE_BUFFER' program instruction is executed.
	Syntax:
	`SEND_COMMAND <DEV>,"'RXON'"`
	Example:
	`SEND_COMMAND RS232_1,"'RXON'"`
	Sets the RS232_1 device to transmit received characters to the Master.

SET BAUD	Set the RS-232/422/485 port's communication parameters.
	Note: *On NX-series controllers, you can use the RS-422/485 ports as 232 ports by using the TSET BAUD command to disable both 422 and 485 modes on the port. When both are disabled on the port, the port operates in 232 mode.*
	Syntax:
	`SEND_COMMAND <DEV>,"'SET BAUD <baud>,<parity>,<data>,<stop> ([422 <Enable | Disable>]'"`
	`SEND_COMMAND <DEV>,"'SET BAUD <baud>,<parity>,<data>,<stop> ([485 <Enable | Disable>]'"`
	Note*: To disable both 422 and 485 modes with one command, end the command with 422/485 Disable.*
	Variables:
	baud = baud rates are: 115200, 76800, 57600, 38400, 19200, 9600, 4800, 2400, 1200, 600, 300, 150.
	parity = N (none), O (odd), E (even), M (mark), S (space).
	data = 8 data bits.
	stop = 1 and 2 stop bits.
	422 Disable = Disables RS-485 mode
	422 Enable = Enables RS-485 mode
	485 Disable = Disables RS-485 mode
	485 Enable = Enables RS-485 mode
	Note*: The only valid 9 bit combination is (baud),N,9,1.*
	Example:
	`SEND_COMMAND RS232_1,"'SET BAUD 115200,N,8,1 485 ENABLE'"`
	Sets the RS232_1 port's communication parameters to 115,200 baud, no parity, 8 data bits, 1 stop bit, and enables RS-485 mode.

SET FAULT DETECT OFF	Disables fault detection on the port. Fault detection is turned on by default.
	Syntax:
	`SEND_COMMAND <DEV>, "’SET FAULT DETECT OFF’"`
	Example:
	`SEND_COMMAND RS232_1,"’SET FAULT DETECT OFF’"`

SET FAULT DETECT ON	Enables fault detection on the port. Fault detection is turned on by default.
	Syntax:
	`SEND_COMMAND <DEV>, "’SET FAULT DETECT ON’"`
	Example:
	`SEND_COMMAND RS232_1,"’SET FAULT DETECT ON’"`

RS-232/422/485 SEND_COMMANDs (Cont.)	
Command	Description

TSET BAUD	Temporarily set the RS-232/422/485 port's communication parameters for a device. TSET BAUD works the same as SET BAUD, except that the changes are not permanent, and the previous values will be restored if the power is cycled on the device.
	Note: *On NX-series controllers, you can use the RS-422/485 ports as 232 ports by using the TSET BAUD command to disable both 422 and 485 modes on the port. When both are disabled on the port, the port operates in 232 mode.*
	Syntax:
	`SEND_COMMAND <DEV>,"'TSET BAUD <baud>,<parity>,<data>,<stop> ([422 <Enable|Disable>]'"`
	`SEND_COMMAND <DEV>,"'TSET BAUD <baud>,<parity>,<data>,<stop> ([485 <Enable|Disable>]'"`
	Note*: To disable both 422 and 485 modes with one command, end the command with 422/485 Disable.*
	Variables:
	baud = baud rates are: 115200, 57600, 38400, 19200, 9600, 4800, 2400, 1200, 600, 300.
	parity = N (none), O (odd), E (even), M (mark), S (space).
	data = 8 or 9 data bits.
	stop = 1 or 2 stop bits.
	422 Disable = Disables RS-422 mode
	422 Enable = Enables RS-422 mode
	485 Disable = Disables RS-485 mode
	485 Enable = Enables RS-485 mode
	Note*: The only valid 9 bit combination is (baud),N,9,1.*
	Example:
	`SEND_COMMAND RS232_1,"'TSET BAUD 115200,N,8,1 485 ENABLE'"`
	Sets the RS232_1 port's communication parameters to 115,200 baud, no parity, 8 data bits, 1 stop bit, and enables RS-485 mode.

TXCLR	Stop and clear all characters waiting in the transmit out buffer and stops transmission.
	Syntax:
	`SEND_COMMAND <DEV>,"'TXCLR'"`
	Example:
	`SEND_COMMAND RS232_1,"'TXCLR'"`
	Clears and stops all characters waiting in the RS232_1 device's transmit buffer.

XOFF	Disable software handshaking (default).
	Syntax:
	`SEND_COMMAND <DEV>,"'XOFF'"`
	Example:
	`SEND_COMMAND RS232_1,"'XOFF'"`
	Disables software handshaking on the RS232_1 device.

XON	Enable software handshaking.
	Syntax:
	`SEND_COMMAND <DEV>,"'XON'"`
	Example:
	`SEND_COMMAND RS232_1,"'XON'"`
	Enables software handshaking on the RS232_1 device.

RS-232/422/485 SEND_STRING Escape Sequences

This device also has some special SEND_STRING escape sequences:

If any of the 3 character combinations below are found anywhere within a SEND_STRING program instruction, they will be treated as a command and not the literal characters.

In these examples: <DEV> = device.

RS-232/422/485 SEND_STRING Escape Sequences

Command	Description

27,17,<time>	Send a break character for a specified duration to a specific device.
	Syntax:
	`SEND_STRING <DEV>,"27,17,<time>"`
	Variable:
	time = 1 - 255. Measured in 100 microsecond increments.
	Example:
	`SEND_STRING RS232_1,"27,17,10"`
	Sends a break character of 1 millisecond to the RS232_1 device.

27,18,0	Clear the ninth data bit by setting it to 0 on all character transmissions.
	Used in conjunction with the 'B9MON' command.
	Syntax:
	`SEND_STRING <DEV>,"27,18,0"`
	Example:
	`SEND_STRING RS232_1,"27,18,0"`
	Sets the RS232_1 device's ninth data bit to 0 on all character transmissions.

27,18,1	Set the ninth data bit to 1 for all subsequent characters to be transmitted.
	Used in conjunction with the 'B9MON' command.
	Syntax:
	`SEND_STRING <DEV>,"27,18,1"`
	Example:
	`SEND_STRING RS232_1,"27,18,1"`
	Sets the RS232_1 device's ninth data bit to 1 on all character transmissions.

27,19,<time>	Insert a time delay before transmitting the next character.
	Syntax:
	`SEND_STRING <DEV>,"27,19,<time>"`
	Variable:
	time = 1 - 255. Measured in 1 millisecond increments.
	Example:
	`SEND_STRING RS232_1,"27,19,10"`
	Inserts a 10 millisecond delay before transmitting characters to the RS232_1 device.

27,20,0	Set the RTS hardware handshake's output to high (> 3V).
	Syntax:
	`SEND_STRING <DEV>,"27,20,0"`
	Example:
	`SEND_STRING RS232_1,"27,20,0"`
	Sets the RTS hardware handshake's output to high on the RS232_1 device.

27,20,1	Set the RTS hardware handshake's output to low/inactive (< 3V).
	Syntax:
	`SEND_STRING <DEV>,"27,20,1"`
	Example:
	`SEND_STRING RS232_1,"27,20,1"`
	Sets the RTS hardware handshake's output to low on the RS232_1 device.

IR/Serial Ports Channels

IR / Serial Ports Channels	
CHANNELS:	Description
00001 - 00229	IR commands.
00229 - 00253	May be used for system call feedback.
00254	Power Fail. (Used w/ 'PON' and 'POF' commands).
00255	Power status. (Shadows I/O Link channel status).
00256 - 65000	IR commands.
65000 - 65534	Future use.

IRRX Port Channels

IRRX Ports Channels	
00001 - 00255	PUSH and RELEASE channels for the received IR code.

IR/Serial SEND_COMMANDs

The following IR and IR/Serial Send_Commands generate control signals for external equipment. In these examples: <DEV> = device.

IR/Serial SEND_COMMANDs	
Command	Description

CAROFF	Disable the IR carrier signal until a 'CARON' command is received.
	Syntax:
	`SEND_COMMAND <DEV>,"'CAROFF'"`
	Example:
	`SEND_COMMAND IR_1,"'CAROFF'"`
	Stops transmitting IR carrier signals to the IR_1 port.

CARON	Enable the IR carrier signals (default).
	Syntax:
	`SEND_COMMAND <DEV>,"'CARON'"`
	Example:
	`SEND_COMMAND IR_1,"'CARON'"`
	Starts transmitting IR carrier signals to the IR_1 port.

IR/Serial SEND_COMMANDs (Cont.)

Command	Description

CH	Send IR pulses for the selected channel. All channels below 100 are transmitted as two digits.
	• If the IR code for ENTER (function #21) is loaded, an Enter will follow the number.
	• If the channel is greater than or equal to (>=) 100, then IR function 127 or 20 (whichever exists) is generated for the one hundred digit.
	• Uses 'CTON' and 'CTOF' times for pulse times.
	Syntax:
	`SEND_COMMAND <DEV>,"'CH',<channel number>"`
	Variable:
	channel number = 0 - 199.
	Example:
	`SEND_COMMAND IR_1,"'CH',18"`
	This device performs the following:
	• Transmits IR signals for 1 (IR code 11). The transmit time is set with the CTON command.
	• Waits until the time set with the CTOF command elapses.
	• Transmits IR signals for 8 (IR code 18).
	• Waits for the time set with the CTOF command elapses. If the IR code for Enter (IR code 21) is programmed, the Controller performs the following steps.
	1) Transmits IR signals for Enter (IR code 21).
	2) Waits for the time set with the CTOF command elapses.

CLEAR FAULT	Forces a reset back to normal status.
	Syntax:
	`SEND_COMMAND <DEV>, "’CLEAR FAULT’"`
	Example:
	`SEND_COMMAND IR_1,"’CLEAR FAULT’"`

CP	Halt and clear all active or buffered IR commands, and then send a single IR pulse.
	Set the Pulse and Wait times with the 'CTON' and 'CTOF' commands.
	Syntax:
	`SEND_COMMAND <DEV>,"'CP',<code>"`
	Variable:
	code = IR port's channel value 0 - 252 (253 - 255 reserved).
	Example:
	`SEND_COMMAND IR_1,"'CP',2"`
	Clears the active/buffered commands and pulses IR_1 port's channel 2.

CTOF	Set the duration of the Off time (no signal) between IR pulses for channel and IR function transmissions. Off time settings are stored in non-volatile memory. This command sets the delay time between pulses generated by the 'CH' or 'XCH' send commands in tenths of seconds.
	Syntax:
	`SEND_COMMAND <DEV>,"'CTOF',<time>"`
	Variable:
	time = 0 - 255. Given in 1/10ths of a second. Default is 5 (0.5 seconds).
	Example:
	`SEND_COMMAND IR_1,"'CTOF',10"`
	Sets the off time between each IR pulse to 1 second.

CTON	Set the total time of IR pulses transmitted and is stored in non-volatile memory. This command sets the pulse length for each pulse generated by the 'CH' or 'XCH' send commands in tenths of seconds.
	Syntax:
	`SEND_COMMAND <DEV>,"'CTON',<time>"`
	Variable:
	time = 0 - 255. Given in 1/10ths of a second. Default is 5 (0.5 seconds).
	Example:
	`SEND_COMMAND IR_1,"'CTON',20"`
	Sets the IR pulse duration to 2 seconds.

IR/Serial SEND_COMMANDs (Cont.)

Command	Description

GET BAUD	Get the IR port’s current DATA mode communication parameters. The port sends the parameters to the device that requested the information. Only valid if the port is in Data Mode (see SET MODE command).
	The port responds with:
	<port #> <baud>,<parity>,<data bits>,<stop bits>
	Syntax:
	`SEND_COMMAND <DEV>,"'GET BAUD'"`
	Example:
	`SEND_COMMAND IR_1,"'GET BAUD'"`
	System response example:
	`PORT 11,9600,N,8,1`

GET FAULT	Check the activation status of fault detection on the port.
	Syntax:
	`SEND_COMMAND <DEV>, "’GET FAULT’"`
	Example:
	`SEND_COMMAND IR_1,"’GET FAULT’"`
	Responds with DISABLED, NONE, SHORT, or NO DEVICE.

GET MODE	Poll the IR/Serial port's configuration parameters and report the active mode settings to the device requesting the information.
	The port responds with: <port #> <mode>,<carrier>,<io link channel>.
	Syntax:
	`SEND_COMMAND <DEV>,"'GET MODE'"`
	Example:
	`SEND_COMMAND IR_1,"'GET MODE"`
	The system could respond with:
	PORT 4 IR,CARRIER,IO LINK 0

GET STATUS	Check the fault detection status of the port.
	Syntax:
	`SEND_COMMAND <DEV>, "’GET STATUS’"`
	Example:
	`SEND_COMMAND IR_1,"’GET STATUS’"`
	Responds with STATUS: NORMAL or STATUS: FAULT.

IROFF	Halt and Clear all active or buffered IR commands being output on the designated port.
	Syntax:
	`SEND_COMMAND <DEV>,"'IROFF'"`
	Example:
	`SEND_COMMAND IR_1,"'IROFF"`
	Immediately halts and clears all IR output signals on the IR_1 port.

POD	Disable previously active 'PON' (power on) or 'POF' (power off) command settings.
	Channel 255 changes are enabled.
	This command is used in conjunction with the `I/O Link` command.
	Syntax:
	`SEND_COMMAND <DEV>,"'POD'"`
	Example:
	`SEND_COMMAND IR_1,"'POD"`
	Disables the 'PON' and 'POF' command settings on the IR_1 device.

IR/Serial SEND_COMMANDs (Cont.)

Command	Description

POF	Turn Off a device connected to an IR port based on the status of the corresponding I/O Link input.
	If at any time the IR sensor input reads that the device is ON (such as if someone turned it on manually at the front panel), IR function 28 (if available) or IR function 9 is automatically generated in an attempt to turn the device back OFF. If three attempts fail, the IR port will continue executing commands in the buffer.
	If there are no commands in the buffer, the IR port will continue executing commands in the buffer and trying to turn the device OFF until a 'PON' or 'POD' command is received. If the IR port fails to turn the device OFF, a PUSH and RELEASE is made on channel 254 to indicate a power failure error. You can only use the 'PON' and 'POF' commands when an IR device has a linked I/O channel. Channel 255 changes are disabled after receipt of this command.
	You can only use the 'PON' and 'POF' commands when an IR device has a linked I/O channel.
	Syntax:
	`SEND_COMMAND <DEV>,"'POF'"`
	Example:
	`SEND_COMMAND IR_1,"'POF'"`
	Sends power down IR commands 28 (if present) or 9 to the IR_1 device.

PON	Turn On a device connected to an IR port based on the status of the corresponding I/O Link input.
	If at any time the IR sensor input reads that the device is OFF (such as if one turned it off manually at the front panel), IR function 27 (if available) or IR function 9 is automatically generated in an attempt to turn the device back ON. If three attempts fail, the IR port will continue executing commands in the buffer and trying to turn the device On.
	If there are no commands in the buffer, the IR port will continue trying to turn the device ON until a 'POF' or 'POD' command is received. If the IR port fails to turn the device ON, a PUSH and RELEASE is made on channel 254 to indicate a power failure error.
	You can only use the 'PON' and 'POF' commands when an IR device has a linked I/O channel. Channel 255 changes are disabled after receipt of this command.
	Syntax:
	`SEND_COMMAND <DEV>,"'PON'"`
	Example:
	`SEND_COMMAND IR_1,"'PON'"`
	Sends power up IR commands 27 or 9 to the IR_1 port.

PTOF	Set the time duration between power pulses in .10-second increments. This time increment is stored in permanent memory. This command also sets the delay between pulses generated by the 'PON' or 'POF' send commands in tenths of seconds. It also sets the delay required after a power ON command before a new IR function can be generated. This gives the device time to power up and get ready for future IR commands.
	Syntax:
	`SEND_COMMAND <DEV>,"'PTOF',<time>"`
	Variable:
	time = 0 - 255. Given in 1/10ths of a second. Default is 15 (1.5 seconds).
	Example:
	`SEND_COMMAND IR_1,"'PTOF',15"`
	Sets the time between power pulses to 1.5 seconds for the IR_1 device.

PTON	Set the time duration of the power pulses in .10-second increments. This time increment is stored in permanent memory. This command also sets the pulse length for each pulse generated by the 'PON' or 'POF' send commands in tenths of seconds.
	Syntax:
	`SEND_COMMAND <DEV>,"'PTON',<time>"`
	Variable:
	time = 0 - 255. Given in 1/10ths of a second. Default is 5 (0.5 seconds).
	Example:
	`SEND_COMMAND IR_1,"'PTON',15"`
	Sets the duration of the power pulse to 1.5 seconds for the IR_1 device.

IR/Serial SEND_COMMANDs (Cont.)

Command	Description

SET BAUD	Set the IR port's DATA mode communication parameters.
	Only valid if the port is in Data Mode (see SET MODE command).
	Syntax:
	`SEND_COMMAND <DEV>,"'SET BAUD <baud>,<parity>,<data>,<stop>'"`
	Variables:
	baud = baud rates are: 19200, 9600, 4800, 2400, and 1200.
	parity = N (none), O (odd), E (even), M (mark), S (space).
	data = 7 or 8 data bits.
	stop = 1 and 2 stop bits.
	Example:
	`SEND_COMMAND IR_1,"'SET BAUD 9600,N,8,1'"`
	Sets the IR_1 port's communication parameters to 9600 baud, no parity, 8 data bits, and 1 stop bit.
	Note: *The maximum baud rate for ports using SERIAL mode is 19200. Also, SERIAL mode works best when using a short cable length (< 10 feet).*

SET FAULT DETECT OFF	Disables fault detection on the port. Fault detection is turned on by default.
	Syntax:
	`SEND_COMMAND <DEV>, "’SET FAULT DETECT OFF’"`
	Example:
	`SEND_COMMAND IR_1,"’SET FAULT DETECT OFF’"`

SET FAULT DETECT ON	Enables fault detection on the port. Fault detection is turned on by default.
	Syntax:
	`SEND_COMMAND <DEV>, "’SET FAULT DETECT ON’"`
	Example:
	`SEND_COMMAND IR_1,"’SET FAULT DETECT ON’"`

SET IO LINK	Link an IR or Serial port to a selected I/O channel for use with the 'DE', 'POD', 'PON', and 'POF' commands.
	The I/O status is automatically reported on channel 255 on the IR port. The I/O channel is used for power sensing (via a PCS or VSS). A channel of zero disables the I/O link.
	Syntax:
	`SEND_COMMAND <DEV>,"'SET IO LINK <I/O number>'"`
	Variable:
	I/O number = 1 - 8. Setting the I/O channel to 0 disables the I/O link.
	Example:
	`SEND_COMMAND IR_1,"'SET IO LINK 1'"`
	Sets the IR_1 port link to I/O channel 1. The IR port uses the specified I/O input as power status for processing 'PON' and 'POF' commands.

SET MODE	Set the IR/Serial ports for IR or Serial-controlled devices to either **IR**, **Serial**, or **Data** mode.
	Syntax:
	`SEND_COMMAND <DEV>, 'SET MODE <mode>'"`
	Variable:
	mode = IR, SERIAL, or DATA.
	Example:
	`SEND_COMMAND IR_1,"'SET MODE IR'"`
	Sets the IR_1 port to IR mode for IR control.
	Note: *The maximum baud rate for ports using SERIAL mode is 19200. Also, SERIAL mode works best when using a short cable length (< 10 feet).*

IR/Serial SEND_COMMANDs (Cont.)

Command	Description

SP	Buffers IR commands which haven't had time to execute yet, and executes each command until the buffer is empty.
	Syntax:
	`SEND_COMMAND <DEV>,"'SP',<code>"`
	Variable:
	code = IR code value 1 - 252 (253-255 reserved).
	Example:
	`SEND_COMMAND IR_1, "'SP',25"`
	Pulses IR code 25 on IR_1 device.

XCH	Transmit the selected channel IR codes in the format/pattern set by the '`XCHM`' send command. Syntax: `SEND_COMMAND <DEV>,"'XCH <channel>'"` Variable: channel = 0 - 9999. Example: For detailed usage examples, refer to the '`XCHM`' command. ***Note:*** *This command supports 4-digit channels.*

IR/Serial SEND_COMMANDs (Cont.)	

XCHM	Changes the IR output pattern for the 'XCH' send command.
	Syntax:
	`SEND_COMMAND <DEV>,"'XCHM-<extended channel mode>'"`
	Variable:
	extended channel mode = 0 - 4.
	Example:
	`SEND_COMMAND IR_1,"'XCHM-3'"`
	Sets the IR_1 device's extended channel command to mode 3.
	Mode 0 Example (default): **[x][x]<x><enter>**
	`SEND_COMMAND IR_1,"'XCH-3'"`
	Transmits the IR code as 3-enter.
	`SEND_COMMAND IR_1,"'XCH-34'"`
	Transmits the IR code as 3-4-enter.
	`SEND_COMMAND IR_1,"'XCH-343'"`
	Transmits the IR code as 3-4-3-enter.
	Mode 1 Example: **<x> <x> <x> <enter>**
	`SEND_COMMAND IR_1,"'XCH-3'"`
	Transmits the IR code as 0-0-3-enter.
	`SEND_COMMAND IR_1,"'XCH-34'"`
	Transmits the IR code as 0-3-4-enter.
	`SEND_COMMAND IR_1,"'XCH-343'"`
	Transmits the IR code as 3-4-3-enter.
	Mode 2 Example: **<x> <x> <x>**
	`SEND_COMMAND IR_1,"'XCH-3'"`
	Transmits the IR code as 0-0-3.
	`SEND_COMMAND IR_1,"'XCH-34'"`
	Transmits the IR code as 0-3-4.
	`SEND_COMMAND IR_1,"'XCH-343'"`
	Transmits the IR code as 3-4-3.
	Mode 3 Example: **[[100][100]...] <x> <x>**
	`SEND_COMMAND IR_1,"'XCH-3'"`
	Transmits the IR code as 0-3.
	`SEND_COMMAND IR_1,"'XCH-34'"`
	Transmits the IR code as 3-4.
	`SEND_COMMAND IR_1,"'XCH-343'"`
	Transmits the IR code as 100-100-100-4-3.
	Mode 4: Mode 4 sends the same sequences as the 'CH' command. Only use Mode 4 with channels 0 - 199.
	Mode 5 Example: **<x><x><x><x><enter>**
	`SEND_COMMAND IR_1,"'XCH-3'"`
	Transmits the IR code as 0-0-0-3-enter.
	`SEND_COMMAND IR_1,"'XCH-34'"`
	Transmits the IR code as 0-0-3-4-enter.
	`SEND_COMMAND IR_1,"'XCH-343'"`
	Transmits the IR code as 0-3-4-3-enter.
	`SEND_COMMAND IR_1,"'XCH-1343'"`
	Transmits the IR code as 1-3-4-3-enter.
	Mode 6 Example: **<x><x><x><x>**
	`SEND_COMMAND IR_1,"'XCH-3'"`
	Transmits the IR code as 0-0-0-3.
	`SEND_COMMAND IR_1,"'XCH-34'"`
	Transmits the IR code as 0-0-3-4.
	`SEND_COMMAND IR_1,"'XCH-343'"`
	Transmits the IR code as 0-3-4-3.
	`SEND_COMMAND IR_1,"'XCH-1343'"`
	Transmits the IR code as 1-3-4-3.

Input/Output SEND_COMMANDs

The I/O port is port 22 on the NX-series controllers.

The following SEND_COMMANDs program the I/O ports on the Integrated Controller.

I/O SEND_COMMANDs

Command	Description

GET DBT	Get Debounce Time
	Syntax:
	`GET DBT <n>`
	Variable:
	n = the channel number of the I/O input port
	Example:
	`SEND_COMMAND 5001:22:0,'GET DBT 1'`
	Retrieves the Debounce time channel 1 on the I/O port.
	Response:
	`DBT 1 50`
	Responds with the channel number and the Debounce time in milliseconds (ms).

SET DBT	Set Debounce Time
	Syntax:
	`SET DBT <n><v>`
	Variables:
	n = the channel number of the I/O input port
	v = Value 1-50 which sets the debounce time in increments of 5ms
	Example:
	`SEND_COMMAND 5001:22:0,'SET DBT 1 10'`
	Sets channel 1 on the I/O port to 50ms Debounce time.

GET INPUT	Get the active state for the selected channels. An active state can be high (logic high) or low (logic low or contact closure). Channel changes, Pushes, and Releases generate reports based on their active state. The port responds with either 'HIGH' or 'LOW'.
	Syntax:
	`SEND_COMMAND <DEV>,"'GET INPUT <channel>'"`
	Variable:
	channel = Input channel 1 - 8.
	Example:
	`SEND_COMMAND IO,"'GET INPUT 1'"`
	Gets the I/O port's active state.
	The system could respond with:
	`INPUT1 ACTIVE HIGH`

SET INPUT	Set the input channel's active state. An active state can be high (logic high) or low (logic low or contact closure). Channel changes, Pushes, and Releases generate reports based on their active state. Setting an input to ACTIVE HIGH will disable the ability to use that channel as an output.
	Syntax:
	`SEND_COMMAND <DEV>,"'SET INPUT <channel> <state>'"`
	Variable:
	channel = Input channel 1 - 8.
	state = Active state HIGH or LOW (default).
	Example:
	`SEND_COMMAND IO,"'SET INPUT 1 HIGH'"`
	Sets the I/O channel to detect a high state change, and disables output on the channel.

PoE SEND_COMMANDs

The NX-4200 has 4 ICSLAN ports, each of which feature Power-over-Ethernet (PoE). The ports are numbered 1-4. The following PoE SEND_COMMANDs program the ICSLAN ports on the controller.

PoE SEND_COMMANDs	
Command	Description

GET CLASS	Retrieve the class type of the device connected via PoE. This command receives a response of ’DISABLED’, ’NO DEVICE’, or ’CLASS x DEVICE’, with x being a value from 0 to 4.
	Syntax:
	`SEND_COMMAND <DEV>,"'GET CLASS'"`
	Example:
	`SEND_COMMAND PoE_24,"'GET CLASS'"`

GET CURRENT	Retrieve the current of the device connected via PoE. This command receives a response with the number in milliamps (mA).
	Syntax:
	`SEND_COMMAND <DEV>,"'GET CURRENT'"`
	Example:
	`SEND_COMMAND PoE_24,"'GET CURRENT'"`

GET FAULT	Retrieve the type of fault on the PoE port. This command receives a response of ’DISABLED’, ’NONE’, ’UNDER-VOLTAGE / OVER-VOLTAGE’, ’CURRENT OVERLOAD’, ’LOAD DISCONNECT’, MAX POWER EXCEEDED,’ or ’POE NOT AVAILABLE’.
	Syntax:
	`SEND_COMMAND <DEV>,"'GET FAULT'"`
	Example:
	`SEND_COMMAND PoE_24,"'GET FAULT'"`

GET STATUS	Retrieve the status of the PoE port. This command receives a response of ’STATUS: NORMAL’ or, ’STATUS: FAULT’.
	Syntax:
	`SEND_COMMAND <DEV>,"'GET STATUS'"`
	Example:
	`SEND_COMMAND PoE_24,"'GET STATUS'"`

GET VOLTAGE	Retrieve the current draw on the PoE port. This command receives a response with the number in volts.
	Syntax:
	`SEND_COMMAND <DEV>,"'GET VOLTAGE'"`
	Example:
	`SEND_COMMAND PoE_24,"'GET VOLTAGE'"`

SET FAULT DETECT OFF	Disables fault detection on the PoE port.
	Syntax:
	`SEND_COMMAND <DEV>,"'SET FAULT DETECT OFF'"`
	Example:
	`SEND_COMMAND PoE_24,"'SET FAULT DETECT OFF'"`

SET FAULT DETECT ON	Enables fault detection on the PoE port.
	Syntax:
	`SEND_COMMAND <DEV>,"'SET FAULT DETECT ON'"`
	Example:
	`SEND_COMMAND PoE_24,"'SET FAULT DETECT ON'"`

SET POWER OFF	Disables PoE to the port. PoE is turned on by default.
	Syntax:
	`SEND_COMMAND <DEV>,"'SET POWER OFF'"`
	Example:
	`SEND_COMMAND PoE_24,"'SET POWER OFF'"`

PoE SEND_COMMANDs (Cont.)	
Command	Description

SET POWER ON	Enables PoE to the port. PoE is turned on by default.
	Syntax:
	`SEND_COMMAND <DEV>,"'SET POWER ON'"`
	Example:
	`SEND_COMMAND PoE_24,"'SET POWER ON'"`

AxLink Commands

The following commands program the AxLink ports on the NX controller.

AxLink SEND_COMMANDs	
Command	Description

AXPWROFF	Powers off the specified AxLink port.
	Syntax:
	`SEND_COMMAND <DEV>,"'AXPWROFF <UPPER|LOWER>'"`
	Variable:
	UPPER|LOWER = Specifies the AxLink port on the controller
	Example:
	`SEND_COMMAND 0,"'AXPWROFF UPPER'"`
	Powers off the upper AxLink port on the controller.

AXPWRON	Powers on the specified AxLink port.
	Syntax:
	`SEND_COMMAND <DEV>,"'AXPWRON <UPPER|LOWER>'"`
	Variable:
	UPPER|LOWER = Specifies the AxLink port on the controller
	Example:
	`SEND_COMMAND 0,"'AXPWRON LOWER'"`
	Powers on the lower AxLink port on the controller.

GET AX FAULT	Retrieve the AxLink port which currently has a fault.
	Syntax:
	`SEND_COMMAND <DEV>,"'GET AX FAULT'"`
	Example:
	`SEND_COMMAND 0,"'GET AX FAULT'"`
	Responds with ’AX FAULT: UPPER/LOWER’ or ’NONE’.

Terminal (Program Port/Telnet) Commands

Overview

There are two types of terminal communications available on NetLinx Integrated Controllers:

- **Program Port** - The "Program" port is a Type-B USB port located on the front panel of the Master that allows terminal communication with the Master. This type of terminal communication requires that you are physically connected to the Master to access the configuration options and commands supported. Since this method of terminal communication requires physical proximity as well as a physical connection to the Master, it is the most secure form of terminal communication.

  For this reason, all Security Configuration options are only available via the Program port (and cannot be accessed via Telnet).
- **Telnet** - This type of terminal communication can be accessed remotely, via TCP/IP. It is a less secure form of terminal communication, since it does not require a physical connection to the Master to connect. Further, the Telnet interface exposes information to the network (which could be intercepted by an unauthorized network client).

***Note:** It is recommended that you make initial configurations as well as subsequent changes via the WebConsole. Refer to the On-Board WebConsole User Interface* section on page 19.

Refer to the *Terminal Commands* section on page 91 for a listing of all commands available in a terminal session.

Note that all commands in the table are available for both Program Port and Telnet sessions, with two exceptions: "Help Security" and "Resetadminpassword". These commands are only available via a Program Port connection.

Establishing a Terminal Connection via the Program Port

To establish a terminal session via the Program Port, the USB port on your PC must be physically connected to the Program port on the NetLinx Master.

Establishing a Terminal Connection via Telnet

1. In your Windows task bar, select **Start > Run** to open the Run dialog.
2. Type **cmd** in the *Open* field and click **OK** to open an instance of the Windows command interpreter (cmd.exe).
3. In the CMD (command), type "**telnet**" followed by a space and the Master’s IP address info.

   Example:

   ```
   >telnet XXX.XXX.XXX.XXX
   ```
4. Press *Enter*.
   - Unless Telnet security is enabled, a session will begin with a welcome banner:

     ```
     Welcome to NetLinx vX.XX.XXX Copyright AMX Corp. 1999-2006
     >
     ```
   - If Telnet security is enabled, type in the word **login** to be prompted for a Username and Password before gaining access to the Master.
5. Enter your username to be prompted for a password.
   - If the password is correct, you will see the welcome banner.
   - If the password is incorrect, the following will be displayed:

     ```
     Login: User1
     Password: *****
     Login not authorized. Please try again.
     ```

   After a delay, another login prompt will be displayed to allow you to try again.

   If after 5 prompts, the login information is not entered correctly, the following message will be displayed and the connection closed:

   ```
   Login not allowed. Goodbye!
   ```

- To restrict access to the Master via terminal connection, enable Configuration Security on the Master via the CONFIGURATION SECURITY option in the Security Options menu - see the *Security Options Menu* section on page 113 for details). With Configuration Security enabled, a valid user with Configuration Security access will have to login before being able to execute Telnet commands. If security is not enabled, these commands are available to all.
- If a connection is opened, but a valid username / password combination is not entered (i.e. just sitting at a login prompt), the connection will be closed after one minute.

Terminal Commands

The Terminal commands listed in the following table can be sent directly to the Master via either a Program Port or a Telnet terminal session (with the exception of the "*Help Security*" and "*Resetadminpassword*" commands, which are only available to a Program Port (RS232) connection.

In your terminal program, type "**Help**" or a question mark ("**?**") and <**Enter**> to access the Help Menu, and display the Program port commands described below:

Terminal Commands	
Command	Description
----- Help ----- <D:P:S>	(Extended diag messages are OFF) `<D:P:S>`: Device:Port:System. If omitted, assumes Master.
? or Help	Displays this list of commands.
AUTO LOCATE (ENABLE|DISABLE|STATUS)	Enables/Disables/queries the auto locate feature on the Master. Auto locate adds additional broadcast information for use by AMX Touch Panel devices configured in *Auto connect* mode.
BOOT STATUS	Returns the current boot state of the master. Response is either "Boot in progress." or "Boot complete."
CLEAR AUDIT LOG	Purges the entire database of audit records. See the *SHOW AUDIT LOG* section on page 104.
CLEAR MAX BUFFERS	Reset the max buffers high-water counters to zero.
CLEAR PERSISTENT VARS	Clear out the persistent/non-volatile variable values without having to download a new NetLinx program.
CPU USAGE	Diagnostic tool to calculate a running average of the current CPU usage of the Master.

DATE	Displays the current date and day of the week.
	Example:
	`>DATE`
	`10/31/2004 Wed`

DATE/TIME ON|OFF	ENABLES/DISABLES the addition of a date time stamp to the terminal logs displayed via "`msg on`" DATE/TIME is Off by default at the start of each Terminal/Telnet session.

DEVICE HOLDOFF ON|OFF	Sets the Master to holdoff devices (i.e. does not allow them to report ONLINE) until all objects in the NetLinx program have completed executing the `DEFINE_START` section.
	If set to `ON`, any messages to devices in `DEFINE_START` will be lost, however, this prevents incoming messages being lost in the Master upon startup.
	When `DEVICE_HOLDOFF` is `ON`, you must use `ONLINE` events to trigger device startup `SEND_COMMANDs`.
	By default, `DEVICE_HOLDOFF` is `OFF` to maintain compatibility with Axcess systems where devices are initialized in `DEFINE_START.`
	***Note**: This command sets the state of the device holdoff. The GET DEVICE HOLDOFF command reveals whether the state is On or Off (see page 93).*
	Example:
	`>Device Holdoff ON`
	`Device Holdoff Set.`

Terminal Commands (Cont.)	
Command	Description
DEVICE STATUS <D:P:S>	Displays a list of all active (on) channels for the specified D:P:S. If you enter `DEVICE STATUS` without the D:P:S variable, the Master displays ports, channels, and version information.
DIPSWITCH	Displays the current state of the Master's hardware dip switches.

DISK FREE	Displays the total bytes of free space available on the Master.
	Example:
	`>DISK FREE`
	` The disk has 2441216 bytes of free space.`

DNS LIST <D:P:S>	Displays the DNS configuration of a specific device including:
	• Domain suffix·
	• Configured DNS IP Information
	Example:
	`>DNS LIST [0:1:0]`
	` Domain suffix:amx.com`
	`  The following DNS IPs are configured`
	`  Entry 1-192.168.20.5`
	`  Entry 2-12.18.110.8`
	`  Entry 3-12.18.110.7`

DOT1X (ENABLE|DISABLE|STATUS)	Enables/disables 802.1x security or displays its current settings. Syntax: `DOT1X[status|enable|disable]`
ECHO ON|OFF	Enables/Disables echo (display) of typed characters.

<table>
<tr><th colspan="2">Terminal Commands (Cont.)</th></tr>
<tr><th>Command</th><th>Description</th></tr>
<tr><td><b>EXPORT (CONFIG|CLONE) TO USB (FRONT|BACK)</b></td><td>Exports a Master's configuration (config) or entire clone to USB media connected to the front or back of the master.
Syntax:
<code>EXPORT [CONFIG|CLONE] TO USB [FRONT|BACK]</code>
The copy format of the configuration export includes:
• Auto-locate enable/disable
• Clock Manager settings
• Device Holdoff setting
• ICSP TCP timeout
• IP Device Discovery enable/disable
• LDAP settings
• Master-to-master route mode
• Message log length
• Message thresholds for threads
• NDP enable/disable
• Queue sizes for threads
• Security configuration including the system, group, and user level settings
• Security Profile
• Server port enable/disable for FTP, HTTP, HTTPS, ICSP, SSH, Telnet
• Server port numbers for FTP, HTTP, HTTPS, ICSP, SSH, Telnet
• SSL certificate parameters
• Startup log enable/disable
• UDP broadcast rate
• zeroconfig enable/disable
The clone format of the configuration export includes all of the items from the copy format plus the following:
• DNS server names
• Domain name
• Duet memory allocation
• Hostname
• System number
• URL list
• NetLinx code
• Java code (Duet modules, XDD modules)
• All user files and folders, (includes .IRL files)
<b><i>Note:</i></b> <i>See IMPORT CONFIG.</i></td></tr>
<tr><td><b>GET DEVICE HOLDOFF</b></td><td>Displays the state of the Master’s device holdoff setting.
<b><i>Note</i></b><i>: This command reveals the state of the device holdoff set using the DEVICE HOLDOFF ON|OFF command (see page 91).</i>
Example:
<code>&gt;GET DEVICE HOLDOFF</code>
<code> Device Holdoff is off.</code></td></tr>
<tr><td><b>GET DUET MEMORY</b></td><td>Display the amount of memory allocated for Duet Java pool. This is the current Java memory heap size as measured in Megabytes. An example is a value of 5 = 5 MB.</td></tr>
<tr><td><b>GET ICSLAN</b></td><td>Displays the current ICSLAN port settings.
Example:
<code>&gt;get icslan</code>
<code>   ICSLan Network: 198.18.0.0</code>
<code>   ICSLan Hostname: ICSLAN</code>
<code>   ICSLan Master IPv4 Address: 198.18.0.1</code>
<code>   ICSLan Master IPv6 Address: fe80::260:9fff:fe98:bd9e</code>
<code>   ICSLan DHCP Server is enabled</code>
<code>   ICSLan Dns Server is 198.18.0.1</code>
<b><i>Note:</i></b> <i>See SET ICSLAN.</i></td></tr>
</table>

Terminal Commands (Cont.)	
Command	Description

GET IP <D:P:S>	Displays the IP configuration of a device.
	If you enter GET IP without the D:P:S variable, the Master displays its D:P:S, Host Name, Type (*DHCP* or *Static*), IP Address, Subnet Mask, Gateway IP, and MAC Address.
	Example:
	`>GET IP [0:1:50]`
	`  IP Settings for 0:1:50`
	`     HostName    MLK-INSTRUCTOR`
	`     Type        DHCP`
	`     IP Address  192.168.21.101`
	`     Subnet Mask 255.255.255.0`
	`     Gateway IP  192.168.21.2`
	`     MAC Address 00:60:9f:90:0d:39`

GET PLATFORM INFO	Retrieves information about a Master connected via USB port. The command returns the master type, host name, system number, IPv4 address, IPv6 address, MAC address, and serial number in a single response.
	Example:
	`>get platform info`
	`DESC=NX-3200;HOST=AMXM98BFB0;SYS=1;IP4=192.168.224.68;IP6=fe80::260:`
	`9fff:fe98:bfb0;MAC=00:60:9f:98:bf:b0;SN='654321',0,0,0,0,0,0,0,0,0`

HELP SECURITY	Displays security related commands.
	Note*: This command is only available to Program Port terminal sessions. It is not available to Telnet sessions (see the Overview* section on page 90*).*
	Example:
	`>HELP SECURITY`
	`>logout   Logout and close secure session`
	`>setup security Access the security setup menus`

ICSPMON ENABLED|DISABLED [PORT]	Enables or disables ICSP monitoring out the specified IP port. By enabling icspmon on an IP port, an external application could connect to that port and "listen" on the ICSP traffic.
IMPORT CONFIG	Installs a previously exported config or clone file. The command searches the USB media for config and clone .tar files and allows you to select which file to import. See *EXPORT (CONFIG|CLONE) TO USB (FRONT|BACK)*.
IMPORT IRL	Loads an IRL file from USB media onto the masters flash file system. The command searches the USB media for .irl files and allows you to select which IRL file to import.
IMPORT KIT	Installs a KIT file from USB media. The command searches the USB media for .kit files and allows you to select which KIT file to import.
IMPORT TKN	Installs a NetLinx token file from USB media. The command searches the USB media for .tkn files and allows you to select which .tkn file to import.

IP STATUS	Provides information about the current NetLinx IP Connections.
	Example:
	`>IP STATUS`
	` NetLinx IP Connections`
	` No active IP connections`

MANAGE FIRMWARE	Telnet interface to load previous and factory firmware versions for both master (device 0) and Integrated Device (device 5001)
	Example:
	`>manage firmware`
	`Devices`
	`-------`
	`0 - Master`
	`5001`
	`  Select device or press return to cancel:0`
	`Current Version:  1.2.259`
	`Previous Version: 1.2.258`
	`Factory Version:  1.2.250`
	` To install a firmware version:`
	`  Enter P (Previous), F (Factory) or press return to cancel:`

Terminal Commands (Cont.)

Command	Description

MEM	Displays the largest free block of the Master’s memory.
	Example:
	`>MEM`
	`The largest free block of memory is 11442776 bytes.`

MSG ON|OFF	Enables/Disables extended diagnostic messages.
	• MSG On [error|warning|info|debug] sets the terminal program to display log messages generated by the Master. The level of log printed to the terminal window depends both on the level used when sending the message and the output level selected with "msg on."
	For example if log output is enabled via "msg on warning" then logs produced at levels AMX_ERROR and AMX_WARNING will be displayed, but not logs produced at levels AMX_INFO or AMX_DEBUG.
	The order of severity from highest to lowest is ERROR, WARNING, INFO, DEBUG.
	If no severity is supplied with "msg on", the default setting is WARNING.
	• MSG OFF disables the display.
	Example:
	`> MSG ON`
	`  Extended diagnostic information messages turned on.`
	`> MSG OFF`
	`  Extended diagnostic information messages turned off.`

MSG STATS	Calculates incoming and outgoing messages over a time interval.

NETLINX LOG LEVEL	Configure the current setting for the NetLinx AMX_LOG facility.
	Example:
	`>netlinx log level`
	`NetLinx Log Level is WARNING`
	`  Set NetLinx Log level to :`
	`    1) ERROR`
	`    2) WARNING`
	`    3) INFO`
	`    4) DEBUG`
	`      Enter selection or press return to keep current level:`
	`>3`
	`NetLinx Log Level set to INFO`

OFF [D:P:S or NAME,CHAN]	Turns off a specified channel on a device. The device can be on any system that the Master you are connected to is able to reach. You can specify the device number, port, and system, or the name of the device that is defined in the `DEFINE_DEVICE` section of the program.
	Syntax:
	`OFF[name,channel]`
	-or-
	`OFF[D:P:S,channel]`
	Example:
	`>OFF[5001:7:4,1]`
	` Sending Off[5001:7:4,1]`

ON [D:P:S or NAME,CHAN]	Turns on a specified channel on a device. The device can be on any system that the Master you are connected to is able to reach. You can specify the device number, port, and system, or the name of the device that is defined in the `DEFINE_DEVICE` section of the program.
	Syntax:
	`ON[name,channel]`
	-or-
	`ON[D:P:S,channel]`
	Example:
	`>ON[5001:7:4,1]`
	` Sending On[5001:7:4,1]`

Terminal Commands (Cont.)

Command	Description

PASS [D:P:S or NAME]	Sets up a pass through mode to a device. In pass through mode, any string received by the device is displayed on the screen, and anything typed is sent as a string to the device. The device can be on any system that the Master you are connected to is able to reach. You can specify the device number, port, and system, or the name of the device that is defined in the `DEFINE_DEVICE` section of the program.
	• Mode is exited by ++ ESC ESC.
	• Display Format is set by ++ ESC n
	Where n =
	A, format = ASCII
	D, format = Decimal
	H = Hex
	Note*: Refer to the ESC Pass Codes* section on page 109 *for detailed descriptions of the supported pass codes.*
	Example:
	`>pass[5001:7:4]`
	` Entering pass mode.`

PHYSICAL STATUS	Retrieve the current LED states.

PING [ADDRESS]	Pings an address (IP or URL), to test network connectivity to and confirms the presence of another networked device. The syntax is just like the PING application in Windows or Linux.
	Example:
	`>ping 192.168.29.209`
	` 192.168.29.209 is alive.`

PROGRAM (ENABLE|DISABLE|STATUS)	Enable/disable the NetLinx program or display the status of the current program execution setting. The PROGRAM command performs the same function as flipping dip switch 1 on the rear panel of the Master. The setting persists until it is manually changed. If the software setting is disabled OR dip switch 1 is "on" then the NetLinx program is disabled. The default setting is enabled. Syntax: `PROGRAM [status|enable|disable]`

PROGRAM INFO	Displays a list of program files and modules residing on the Master.
	Example:
	`>PROGRAM INFO`
	` -- Program Name Info`
	` -- Module Count = 1`
	`      1   Name is i!-PCLinkPowerPointTest`
	
	` -- File Names = 2`
	`      1 = C:\Program Files\AMX Applications\i!-PCLinkPowerPoint`
	`      2 = C:\Program Files\Common Files\AMXShare\AXIs\NetLinx.axi`
	`      2 = Name is MDLPP`
	
	` -- File Names = 2`
	`      1 C:\AppDev\i!-PCLink-PowerPoint\i!-PCLinkPowerPointMod.axs`
	`      2 C:\Program files\Common Files\AMXShare\AXIs\NetLinx.axi`

PULSE [D:P:S or NAME,CHAN]	Pulses a specified channel on a device on and off. The device can be on any system the Master you are connected to can reach. You can specify the device number, port, and system; or the name of the device that is defined in the `DEFINE_DEVICE` section of the program.
	Example:
	`>PULSE[50001:8:50,1]`
	`Sending Pulse[50001:8:50,1]`

PWD	Displays the name of the current directory.
	Example:
	`pwd`
	`      The current directory is doc:`

Terminal Commands (Cont.)

Command	Description

REBOOT	Reboots the Master or specified device. Options for rebooting the Master are cold, soft, and warm. The reboot command with no parameter executes as "reboot cold".
	Example (Rebooting device):
	`>REBOOT [0:1:0]`
	` Rebooting...`
	Example (Rebooting Master):
	`>reboot cold`
	Reboots the Master and restarts the entire operating system.
	`>reboot warm`
	`>reboot soft`
	Reboots the Master but only starts the AMX NetLinx application firmware.

RENEW DHCP	Renews/Releases the current DHCP lease for the Master. ***Note**: The Master must be rebooted to acquire a new DHCP lease.* Example: `>RENEW DHCP`
RESETADMINPASSWORD	This command resets the administrator password back to "password". ***Note**: This command is only available to Program Port terminal sessions. It is not available to Telnet sessions (see the Overview* section on page 90*).*
RESET FACTORY	Resets the Master to factory default state including removal of all security settings, removal of all user files, resetting to DHCP, and loading an empty NetLinx program. The Master will be effectively in an out-of-box state.

ROUTE MODE DIRECT|NORMAL	Sets the Master-to-Master route mode:
	• Normal mode - allows a Master to communicate with any Master accessible via the routing tables (shown with the `SHOW ROUTE` command - see page 107). This includes a directly-connected Master (route metric =1) and indirectly connected Masters (route metric greater than 1, but less than 16).
	• Direct mode - allows communication only with Masters that are directly connected (route metric = 1). Indirectly connected Masters cannot be communicated within this mode.
	Examples:
	`>ROUTE MODE DIRECT`
	` Route Mode "Direct" Set`
	`>ROUTE MODE NORMAL`
	` Route Mode "Normal" Set`

SEND_COMMAND D:P:S or NAME,COMMAND	Sends a specified command to a device. The device can be on any system that the Master you are connected to can reach. You can specify the device number, port, and system; or the name of the device that is defined in the `DEFINE_DEVICE` section of the Program.
	The data of the string is entered with the following NetLinx string syntax:
	`SEND_COMMAND 1:1:1,"'This is a test',13,10"`
	`SEND_COMMAND RS232_1,"'This is a test',13,10"`

SEND_LEVEL <D:P:S>, <LEVEL ID>,<LEVEL VALUE>	Allows the user to set a level on a device via the Master's Telnet/ program port interface.
SEND_STRING D:P:S or NAME,STRING	Sends a string to a specified device. The device can be on any system that the Master you are connected to can reach. You can specify the device number, port, and system; or the name of the device defined in the `DEFINE_DEVICE` section of the Program. The data of the string is entered with NetLinx string syntax.

<table>
<tr><th colspan="2">Terminal Commands (Cont.)</th></tr>
<tr><th>Command</th><th>Description</th></tr>
<tr><td><b>SET DATE</b></td><td>

Prompts you to enter the new date for the Master. When the date is set on the Master, the new date will be reflected on all devices in the system that have clocks (i.e. touch panels). By the same token, if you set the date on any system device, the new date will be reflected on the system’s Master, and on all connected devices.

***Note**: This command will not update clocks on devices connected to another Master (in Master-to-Master systems).*

Example:

```
>SET DATE
 Enter Date: (mm/dd//yyyy) ->
```

</td></tr>
<tr><td><b>SET DNS <D:P:S&gt;</b></td><td>

Sets up the DNS configuration of a device. This command prompts you to enter a Domain Name, DNS IP #1, DNS IP #2, and DNS IP #3. Then, enter Y (yes) to approve/store the information in the Master.

Entering N (no) cancels the operation.

***Note**: The device must be rebooted to enable new settings.*

Example:

```
>SET DNS [0:1:0]
-- Enter New Values or just hit Enter to keep current settings --

  Enter Domain Suffix: amx.com
  Enter DNS Entry 1  : 192.168.20.5
  Enter DNS Entry 2  : 12.18.110.8
  Enter DNS Entry 3  : 12.18.110.7

  You have entered: Domain Name: amx.com
                   DNS Entry 1: 192.168.20.5
                   DNS Entry 2: 12.18.110.8
                   DNS Entry 3: 12.18.110.7

  Is this correct? Type Y or N and Enter -> Y
  Settings written. Device must be rebooted to
  enable new settings
```

</td></tr>
<tr><td><b>SET DUET MEMORY</b></td><td>

Set the amount of memory allocated for Duet Java pool. This is the current Java memory heap size as measured in Megabytes. This feature is used so that if a NetLinx program requires a certain size of memory be allotted for its currently used Duet Modules, it can be reserved on the target Master.

Valid values are:

- 2 - 8 for 32MB systems
- 2 - 36 for 64MB systems.

This setting does not take effect until the next reboot.

***Note:** If you are trying to accomplish this setting of the Duet Memory size via a NetLinx program, the program command "DUET_MEM_SIZE_SET(int)" should call REBOOT() following a set.*

</td></tr>
<tr><td><b>SET FTP PORT</b></td><td>

Enables/Disables the Master’s IP port listened to for FTP connections.

***Note**: The Master must be rebooted to enable new settings.*

Example:

```
>SET FTP PORT
 FTP is enabled
 Do you want to enable (e) or disable (d) FTP (enter e or d):
 FTP enabled, reboot the Master for the change to take
 affect.
```

</td></tr>
<tr><td><b>SET HTTP PORT</b></td><td>

Sets the Master’s IP port listened to for HTTP connections.

***Note**: The Master must be rebooted to enable new settings.*

Example:

```
>SET HTTP PORT
 Current HTTP port number = 80
 Enter new HTTP port number (Usually 80) (0=disable HTTP):
 Setting HTTP port number to
 New HTTP port number set, reboot the Master for the change to take
 affect.
```

</td></tr>
</table>

Terminal Commands (Cont.)

Command	Description

SET HTTPS PORT	Sets the Master's IP port listened to for HTTPS connections.
	***Note**: The Master must be rebooted to enable new settings.*
	Example:
	`>SET HTTPS PORT`
	`Current HTTPS port number = 443`
	`Enter new HTTPS port number (Usually 443) (0=disable HTTPS):`
	Once you enter a value and press the ENTER key, you get the following message:
	`Setting HTTPS port number to`
	`New HTTPS port number set, reboot the Master for`
	`the change to take affect.`

SET ICSLAN	Sets the ICSLAN port settings.
	Example:
	`>set icslan`
	`--- Enter New Values or just hit Enter to keep current settings`
	`Enter ICSLan Host Name:    ICSLAN`
	`Enter ICSLan Network octet 1:    198`
	`Enter ICSLan Network octet 2:    18`
	`Disable DHCP Server? (Y):`

SET ICSP PORT	Sets the Master's IP port listened to for ICSP connections.
	***Note**: The Master must be rebooted to enable new settings.*
	Example:
	`>SET ICSP PORT`
	`Current ICSP port number = 1319`
	`Enter new ICSP port number (Usually 1319)`
	`(0=disable ICSP):`
	Once you enter a value and press the ENTER key, you get the following message:
	`Setting ICSP port number to`
	`New ICSP port number set, reboot the Master for the`
	`change to take affect.`

SET ICSP TCP TIMEOUT	Sets the timeout period for ICSP and i!-Web Control TCP connections.
	***Note**: The new timeout value is immediately (no reboot required).*
	Example:
	`>SET ICSP TCP TIMEOUT`
	
	`This will set the timeout for TCP connections for both ICSP and i!-Web`
	`Control.When no communication has been detected for the specified`
	`number of seconds, the socket connection is closed.ICSP and i!-Web`
	`Control have built-in timeouts and reducing the TCP timeout below`
	`these will cause undesirable results. The default value is 45`
	`seconds.`
	
	`The current ICSP TCP timeout is 45 seconds`
	`Enter new timeout (in seconds):`
	Once you enter a value and press the ENTER key, you get the following message:
	`New timeout value set (in affect immediately).`

<table>
<tr><th colspan="2">Terminal Commands (Cont.)</th></tr>
<tr><th>Command</th><th>Description</th></tr>
<tr><td><b>SET IP &lt;D:P:S&gt;</b></td><td>
<p>Sets the IP configuration of a specified device.</p>
<p>Enter a Host Name, Type (DHCP or Fixed), IP Address, Subnet Mask, and Gateway IP Address.</p>
<p><b><i>Note</i></b><i>: For NetLinx Central Controllers, the "Host Name" can only consist of alphanumeric characters.</i></p>
<ul><li>Enter Y (yes) to approve/store the information into the Master.</li>
<li>Enter N (no) to cancel the operation.</li></ul>
<p><b><i>Note</i></b><i>: The Device must be rebooted to enable new settings.</i></p>
<p>Example:</p>
<pre>
>SET IP [0:1:0]
 --- Enter New Values or just hit Enter to keep current settings ---

 Enter Host Name: MLK-INSTRUCTOR
 Enter IP type. Type D for DHCP or S for Static IP and then Enter:
DHCP
 Enter Gateway IP: 192.168.21.2

 You have entered: Host Name   MLK-INSTRUCTOR
                   Type   DHCP
                   Gateway IP 192.168.21.2
 Is this correct? Type Y or N and Enter -> y
 Settings written. Device must be rebooted to enable new settings.
</pre>
</td></tr>
<tr><td><b>SET LOG COUNT</b></td><td>
<p>Sets the number of entries allowed in the message log.</p>
<p><b><i>Note</i></b><i>: The Master must be rebooted to enable new settings.</i></p>
<p>Example:</p>
<pre>
>SET LOG COUNT
  Current log count = 1000
  Enter new log count (between 50-10000):
</pre>
<p>Once you enter a value and press the ENTER key, you get the following message:</p>
<pre>
  Setting log count to
  New log count set, reboot the Master for the change to
  take affect.
</pre>
</td></tr>
<tr><td><b>SET QUEUE SIZE</b></td><td>
<p>Provides the capability to modify maximum message queue sizes for various threads.</p>
<p>Example:</p>
<pre>
set queue size
</pre>
<p>This will set the maximum message queue sizes for several threads.</p>
<p>Use caution when adjusting these values.</p>
<p>Set Queue Size Menu:</p>
<p>1. Interpreter (factory default=2000, currently=600)
2. Notification Manager (factory default=2000, currently=200)
3. Connection Manager (factory default=2000, currently=500)
4. Route Manager (factory default=400, currently=200)
5. Device Manager (factory default=500, currently=500)
6. Diagnostic Manager (factory default=500, currently=500)
7. TCP Transmit Threads (factory default=600, currently=200)
8. IP Connection Manager (factory default=800, currently=500)
9. Message Dispatcher (factory default=1000, currently=500)
10. Axlink Transmit (factory default=800, currently=200)
11. PhastLink Transmit (factory default=500, currently=500)
12. ICSNet Transmit (factory default=500, currently=500)
13. ICSP 232 Transmit (factory default=500, currently=500)
14. UDP Transmit (factory default=500, currently=500)
15. NX Device (factory default=500, currently=500)</p>
<p>Enter choice or press ESC.</p>
</td></tr>
</table>

Terminal Commands (Cont.)	
Command	Description

SET SECURITY PROFILE	Sets a pre-defined Security Profile (a grouped set of security settings). The Security Profile can be set to *"none" (default setting)*, "*Secure*", or "*DOD*" (see below).
	***Note**: The Security Profile can only be configured via the terminal interface of the Master's Program port.*
	Example:
	`set security profile`
	When you press Enter, the system responds with:
	`Current Security Profile = 0 (none)`
	`Enter new security profile (0=none, 1=secure, 2=DOD):`
	Once you enter a value and press Enter, the system responds with:
	`New security profile set, reboot the Master for change to fully take effect.`
	The three Security Profiles are described below:
	None (default):
	• No security is enabled and all Master interface ports are available including HTTP, HTTPS, Telnet, SSH, FTP and terminal access.
	• Logins are not required on the Master's Web, Telnet and terminal interfaces.
	This is the default out-of-the-box configuration.**Secure:**
	• Unsecured interface ports are disabled including HTTP, Telnet and FTP. Only HTTPS and SSH and terminal user ports are available.
	• All user access requires a username/password login including HTTPS, SSH and terminal.
	• NetLinx/ICSP security is enabled requiring all NetLinx devices connecting with the Master to provide username/password authentication and encryption.
	• Passwords must conform to a stricter set of requirements. They must be at least 8 characters long and contain at least one upper and one lower case alpha, one numeric and one special character (excluding the blankspace).
	Allowed Special Characters:
	The following special characters are allowed for use in User Name and Password entries:
	! " # $ % & ' ( ) * + , - . / : ; < = > ? @ [\ ] ^ _ ` { | } ~
	Also allowed are any printable ASCII characters (including "*space*"): **A-Z**, **a-z**, **0-9**.
	• Passwords cannot contain back-to-back duplicate characters.
	• To ensure all account passwords conform to the new standard, all existing user accounts are deleted and the built-in 'administrator' and 'netlinx' account passwords are set to the secure default of 'Amx1234!'
	• Failed login attempts will force a 4 second delay before a subsequent login attempt can occur.
	• Three consecutive login failures from any location will cause a 15 minute lockout for the specified user account.
	• If a banner.txt file is present in the Master's /user directory, the text from the banner.txt file will be included on the Master's Web login prompt.
	• All user account access will be timed out after at most 15 minutes of inactivity by the user. Any activity after the timeout will cause the login prompt to be displayed and login will be required to regain access. The inactivity timer on an SSH and terminal session will be disabled if "msg on" logging is active.
	• All account access including successful and failed logins and logouts will be recorded in persistent storage. Audit records will be retained for 90 days. The current audit logs can be viewed via SSH or terminal sessions using the "show audit log" command. The audit log can be manually cleared from SSH or terminal session using the "clear audit log" command.

Terminal Commands (Cont.)

<table>
<tr><th>Command</th><th>Description</th></tr>
<tr><td>SET SECURITY PROFILE (Cont.)</td><td>

DoD:

DoD security profile has all of the security specifications of "secure" profile along with the following additional features:

- The default Web login banner text consists of the following: "*This is a Department of Defense (DOD) computer system provided only for authorized U.S. Government use. This system may be monitored for all lawful purposes. All information, including personal information, placed on or sent over this system, may be monitored. Use of this DOD computer system, authorized or unauthorized, constitutes consent to monitoring of this system. Unauthorized use may subject you to criminal prosecution and penalties.*"
- The default Web login banner text can be overridden by providing a banner.txt file in the /user directory.
- The SSH and terminal interface will display the following banner after a successful login: "*DOD use only! Subject to monitoring, reporting, prosecution, and penalties.*"

Secure and DoD profile configuration can be tailored with more or less security features by manually altering the Master's configuration following the secure profile selection. For example, the Master can be put into "secure" profile and then the HTTP and Telnet interfaces can be manually re-enabled via their existing configuration mechanism. This would enable all of the new security features provided by the "secure" profile but still allow Master access via HTTP and Telnet.

***Note**: When transitioning from secure or DoD profile to the "non" profile, user accounts are NOT wiped and the "administrator" and "netlinx" accounts will retain their secure passwords.*

</td></tr>
<tr><td>

SET SNMP

</td><td>

Sets SNMP read and write community strings. This command invokes the SET SNMP sub-menu:

```
>SET SNMP
--- Enter New Values or just hit Enter to keep current settings
SNMP Enabled (Y or N)? N  y
Enter System Description:     NetLinx VxWorks SNMPv1/v2c Agent
Enter System Contact:         AMX LLC
Enter System Location:        Richardson, TX USA
Enter Read community string:  public
Enter Write community string: private
```

You have entered:

```
Description = NetLinx VxWorks SNMPv1/v2c Agent
Contact = AMX LLC
Location = Richardson, TX USA
Read Community = public
Write Community = private

Is this correct? Type Y or N and Enter->
```

***Note**: The "System Description", "System Contact" and "System Location" are the values that will be published for the Master via SNMP. The system must be rebooted once the new values are entered.*

</td></tr>
<tr><td>

SET SSH PORT

</td><td>

Sets the Master’s IP port listened to for SSH connections.

***Note**: The Master must be rebooted to enable new settings.*

Example:

```
>SET SSH PORT
  Current SSH port number = 22
  Enter new SSH port number (Usually 22) (0=disable SSH):
```

Once you enter a value and press the ENTER key, you get the following message:

```
Setting SSH port number to 22
New SSH port number set, reboot the Master for   the change to take
effect.
```

</td></tr>
</table>

Terminal Commands (Cont.)

Command	Description

SET SYSTEM NUMBER	Sets the system number for this Master. A reboot of the Master following the execution of this command is required for the change to take effect.
	Example:
	`>set system number`
	`Current System number = 1`
	`Enter new System number : 2`
	`Setting System number to 2`
	New System number set, reboot the master for the change to take effect.

SET TELNET PORT	Sets the Master's IP port listened to for Telnet connections.
	Note*: The Master must be rebooted to enable new settings.*
	Example:
	`>SET TELNET PORT`
	` Current telnet port number = 23`
	` Enter new telnet port number (Usually 23)`
	` (0=disable Telnet):`
	Once you enter a value and press the ENTER key, you get the following message:
	`Setting telnet port number to 23`
	`New telnet port number set, reboot the Master for the change to take effect.`

SET THRESHOLD	Sets the Master's internal message thresholds.
	This command will set the thresholds of when particular tasks are pended. The threshold is the number of messages queued before a task is pended.
	Use extreme caution when adjusting these values.
	Note*: The Master must be rebooted to enable new settings.*
	Example:
	`>SET THRESHOLD`
	
	`-- This will set the thresholds of when particular tasks are pended. The threshold is the number of messages queued before a task is pended.--`
	`--Use extreme caution when adjusting these values.--`
	`  Current Interpreter Threshold = 2000`
	`  Enter new Interpreter Threshold (Between 1 and 2000)(Default=10):`
	Once you enter a value and press the ENTER key, you get the following message:
	`  Current Lontalk Threshold = 50`
	`  Enter new Lontalk Threshold (Between 1 and 2000)`
	`   (Default=50):50`
	`  Current IP Threshold = 600`
	`  Enter new IP Threshold (Between 1 and 2000)`
	`  (Default=200): 600`
	`  Setting Thresholds to: Interpreter 2000`
	`                         Lontalk     50`
	`                         IP          600`
	`New thresholds set, reboot the Master for the changes to take effect.`

SET TIME	Sets the current time. When the time is set on the Master, the new time will be reflected on all devices in the system that have clocks (i.e. touch panels). By the same token, if you set the time on any system device, the new time will be reflected on the system's Master, and on all connected devices.
	Note*: This will not update clocks on devices connected to another Master (in Master-to-Master systems).*
	Example:
	`>SET TIME`
	` Enter Date: (hh:mm:ss) ->`

SET TIMELINE LOOPCNT	Sets the Master's timeline/event max loopcount.

Terminal Commands (Cont.)	
Command	Description

SET UDP BC RATE	Sets the UDP broadcast rate. A broadcast message is sent by the Master to allow devices to discover the Master. This command allows the broadcast frequency to be changed or eliminate the broadcast message.
	Example:
	`>SET UPD BC RATE`
	` Current broadcast message rate is 5 seconds between messages.`
	`  Enter broadcast message rate in seconds between messages`
	` (off=0 ; default=5) (valid values 0-300):`
	Once you enter a value and press the ENTER key, you get the following message:
	`Setting broadcast message rate to 300 seconds between messages`
	`New broadcast message rate set.`

SET URL <D:P:S>	Sets the initiated connection list URLs of a device. Enter the URL address and port number of another Master or device (that will be added to the URL list).
	• Enter Y (yes) to approve/store the new addresses in the Master.
	• Enter N (no) to cancel the operation.
	Example:
	`>SET URL [0:1:0]`
	`     No URLs in the URL connection list`
	` Type A and Enter to Add a URL or Enter to exit.`
	`> a`
	
	` Enter URL -> 192.168.21.200`
	` Enter Port or hit Enter to accept default (1319) ->`
	` Enter Type (Enter for permanent or T for temporary) ->`
	`     URL Added successfully.`

SHOW AUDIT LOG	Displays the User Account Access Audit Log.
	Example:
	`SHOW AUDIT LOG`
	`08-24-2009 06:54:04 <TERMINAL> administrator TERMINAL LOGIN_SUCCESS`
	`08-24-2009 07:05:30 <TERMINAL> administrator TERMINAL LOGIN_SUCCESS`
	`09-04-2009 09:21:09 <TERMINAL> administrator TERMINAL LOGIN_SUCCESS`
	`09-04-2009 09:25:49 192.168.220.171 administrator HTTPS LOGIN_SUCCESS`
	`09-04-2009 09:35:55 192.168.220.171 administrator HTTPS LOGOUT`
	`09-08-2009 06:07:46 192.168.220.171 administrator SSH LOGIN_SUCCESS`
	`09-08-2009 06:07:55 192.168.220.171 administrator SSH LOGOUT`
	`09-08-2009 07:44:29 192.168.220.171 administrator HTTPS LOGIN_FAIL`
	`09-08-2009 07:44:44 192.168.220.171 administrator HTTPS LOGIN_SUCCESS`
	`09-08-2009 07:45:25 192.168.220.171 administrator HTTPS LOGOUT`
	Each record displays:
	• Date and time of access,
	• Connection source consisting of either `<TERMINAL>` or the IP address of the user,
	• Account username,
	• Access transport mechanism (`TERMINAL`, `HTTP`, `HTTPS`, `TELNET`, `SSH`)
	• Activity (`LOGIN_SUCCESS`, `LOGIN_FAIL`, `LOGOUT`).
	***Note**: Records older than 90 days will be automatically purged.*
	The entire database of audit records can be purged manually from Telnet/SSH/ terminal session using the "`CLEAR AUDIT LOG`" command (see page 91).

<table>
<tr><th colspan="2">Terminal Commands (Cont.)</th></tr>
<tr><th>Command</th><th>Description</th></tr>
<tr><td><b>SHOW BUFFERS</b></td><td>Displays a list of various message queues and the number of buffers in each queue
Example:
<pre>
show buffers
Thread   TX   RX   Queued
----------- ----   ----   ----
Axlink   0
UDP   0   0-Sent=NO Waiting=NO
IPCon Mgr   0

Con Manager   0
Interpreter   0
Device Mgr   0
Diag Mgr   0
Msg Dispatch   0
Cfg Mgr   0
Route Mgr   0
Notify Mgr   0
            ----   ----   ----
Total   0   0   0 GrandTotal 0
</pre>
<b><i>Note</i></b>: <i>See the SHOW MAX BUFFERS</i> section on page 107.</td></tr>
<tr><td><b>SHOW COMBINE</b></td><td>Displays a list of devices, levels, and channels that are currently combined.
Example:
<pre>
> SHOW COMBINE
  Combines

  Combined Device([33096:1:1],[96:1:1])
  Combined Level([33096:1:1,1],[128:1:1,1],[10128:1:1,1])
  Combined Device([33128:1:1],[128:1:1],[10128:1:1])
</pre></td></tr>
<tr><td><b>SHOW DEVICE <D:P:S&gt;</b></td><td>Displays a list of devices present on the bus, with their device attributes.
Example:
<pre>
>SHOW DEVICE [0:1:0]
Local devices for system #1 (This System)

Device (ID)Model   (ID)Mfg   FWID Version
00000 (00256)NXC-ME260/64M   (00001)AMX Corp.   00336 v3.00.312
       (PID=0:OID=0) Serial=0,0,0,0,0,0,0,0,0,0,0,0,
       Physical Address=NeuronID 000531589201
        (00256)vxWorks Image   (00001)   00337 v3.00.312
         (PID=0:OID=1) Serial=N/A
        (00256)BootROM   (00001)   00338 v3.00.312
         (PID=0:OID=2) Serial=N/A
         (00256)AXlink I/F uContr(00001)   00270 v1.03.14
         (PID=0:OID=3) Serial=0000000000000000
</pre></td></tr>
</table>

<table>
<tr><th colspan="2">Terminal Commands (Cont.)</th></tr>
<tr><th>Command</th><th>Description</th></tr>
<tr><td><b>SHOW LOG</b></td><td>
Displays the log of messages stored in the Master's memory. The Master logs all internal messages and keeps the most recent messages. The log contains:

- Entries starting with first specified or most recent
- Date, Day, and Time message was logged
- Which object originated the message
- The text of the message:

<pre>
SHOW LOG [start] [end]
SHOW LOG ALL
</pre>

- <start> specifies message to begin the display.

- If start is not entered, the most recent message will be first.

- If end is not entered, the last 20 messages will be shown.

- If <ALL> is entered, all stored messages will be shown, starting with the most recent.

Example:

<pre>
>SHOW LOG
 Message Log for System 50 Version: v2.10.75
 Entry   Date/Time   Object   Text

  1: 11-01-2001 THU 14:14:49 ConnectionManager
     Memory Available = 11436804 <26572>
  2: 11-01-2001 THU 14:12:14 ConnectionManager
     Memory Available = 11463376 <65544>
  3: 11-01-2001 THU 14:10:21 ConnectionManager
     Memory Available = 11528920 <11512>
  4: 11-01-2001 THU 14:10:21 TelnetSvr
 Accepted Telnet connection:socket=14 addr=192.168.16.110
 port=2979
  5: 11-01-2001 THU 14:05:51 Interpreter
     CIpEvent::OnLine 10002:1:50
  6: 11-01-2001 THU 14:05:51 Interpreter
     CIpEvent::OnLine 128:1:50
  7: 11-01-2001 THU 14:05:51 Interpreter
     CIpEvent::OffLine 128:1:50
  8: 11-01-2001 THU 14:05:51 Interpreter
     CIpEvent::OnLine 96:1:50
  9: 11-01-2001 THU 14:05:51 Interpreter
     CIpEvent::OffLine 96:1:50
 10: 11-01-2001 THU 14:05:51 Interpreter
     CIpEvent::OnLine 128:1:50
 11: 11-01-2001 THU 14:05:51 Interpreter
     CIpEvent::OnLine 96:1:50
 12: 11-01-2001 THU 14:05:51 Interpreter
     CIpEvent::OnLine 5001:16:50
 13: 11-01-2001 THU 14:05:51 Interpreter
     CIpEvent::OnLine 5001:15:50
 14: 11-01-2001 THU 14:05:51 Interpreter
</pre>

To display only the startup log, use the SHOW START LOG command (see page 108).
</td></tr>
</table>

<table>
<tr><th colspan="2">Terminal Commands (Cont.)</th></tr>
<tr><th>Command</th><th>Description</th></tr>
<tr><td>

SHOW MAX BUFFERS

</td><td>

Displays a list of various message queues and the maximum number of message buffers that were ever present on the queue.

Example:

```
show max buffers
Thread       TX   RX
----------- ---- ----
Axlink         1
UDP            1
IPCon Mgr      0 (Total for TCP Connections TX=0)

Con Manager         8
Interpreter        17
Device Mgr          8
Diag Mgr            1
Msg Dispatch        0
Cfg Mgr             0
Route Mgr           0
Notify Mgr          0
            ----   ----  ----
Total          2   34    GrandTotal 36
```

See the *SHOW BUFFERS* section on page 105.

</td></tr>
<tr><td>

SHOW MEM

</td><td>

Displays the memory usage for all memory types.

</td></tr>
<tr><td>

SHOW NOTIFY

</td><td>

Displays the Notify Device List (Master-Master). This is a list of devices (up to 1000) that other systems have requested input from and the types of information needed.

Note*: The local system number is* ***1061****.*

Example:

```
>SHOW NOTIFY

 Device Notification List of devices requested by other Systems

    Device:Port   System  Needs
    ------------------------------------------------------
    00128:00001   00108   Channels Commands Strings Levels
    33000:00001   00108   Channels Commands
```

</td></tr>
<tr><td>

SHOW REMOTE

</td><td>

Displays the Remote Device List (Master-Master). This is a list of the devices this system requires input from and the types of information needed. If when a NetLinx Master connects to another NetLinx Master, the newly connecting system has a device that the local system desires input from; the new system is told what information is desired from what device.

Note*: The local system number is* ***1062****.*

Example:

```
>SHOW REMOTE

 Device List of Remote Devices requested by this System

   Device  Port  System  Needs
   ------------------------------------------------------
   00001  00001  00001   Channels Commands
   00002  00001  00001   Channels Commands
   33000  00001  00001   Channels Commands
   00128  00001  00108   Channels Commands Strings Levels
   33000  00001  00108   Channels Commands
```

</td></tr>
<tr><td>

SHOW ROUTE

</td><td>

Displays information about how this NetLinx Master is connected to other NetLinx Masters (routing information).

Example:

```
>SHOW ROUTE
   Route Data:

   System Route  Metric  PhyAddress
   --------------------------------
  -> 50     50      0      AxLink
```

</td></tr>
</table>

<table>
<tr><th colspan="2">Terminal Commands (Cont.)</th></tr>
<tr><th>Command</th><th>Description</th></tr>
<tr><td><b>SHOW START LOG <START&gt;</b></td><td>Displays the startup log (see <code>START LOG</code> below).
<START> specifies the message to begin the display.
'ALL' will display all startup log messages.
<i><b>Note</b>: This command is identical in implementation to the SHOW LOG command (see page 106), except that it executes the startup log.</i></td></tr>
<tr><td><b>SHOW SYSTEM &lt;S&gt;</b></td><td>Displays a list of all devices in all systems currently on-line. The systems lists are either directly connected to this Master (i.e. 1 hop away), or are referenced in the <code>DEFINE_DEVICE</code> section of the NetLinx program. Optionally, you may provide the desired system number as a parameter to display only that system's information (e.g. <code>SHOW SYSTEM 2001</code>).
The systems listed are in numerical order.
Example:
<pre>
>SHOW SYSTEM
 Local devices for system #50 (This System)

Device (ID)Model   (ID)Mfg   FWID   Version
00000 (00256)Master   (00001)AMX Corp.   00256   v2.10.75
       (PID=0:OID=0) Serial='2010-12090',0,0,0,0,0,0
       Physical Address=NeuronID 000239712501
         (00256)vxWorks Image   (00001)   00257   v2.00.77
         (PID=0:OID=1) Serial=N/A
         (00256)BootROM   (00001)   00258   v2.00.76
         (PID=0:OID=2) Serial=N/A
         (00256)AXlink I/F uContr(00001)   00270   v1.02
         (PID=0:OID=3) Serial=0000000000000000
 00096 (00192)VOLUME 3 CONTROL BO(00001)AMX Corp. 00000   v2.10
       (PID=0:OID=0) Serial=0000000000000000
       Physical Address=Axlink
 00128 (00188)COLOR LCD TOUCH PAN(00001)AMX Corp. 32778   v5.01d
       (PID=0:OID=0) Serial=0000000000000000
       Physical Address=Axlink
 05001 (00257)NXI Download   (00001)AMX Corp. 00260   v1.00.20
       (PID=0:OID=0) Serial=0,0,0,0,0,0,0,0,0,0,0,0,
       Physical Address=NeuronID 000189145801
         (00257)NXI/NXI-1000 Boot(00001)   00261   v1.00.00
         (PID=0:OID=1) Serial=0,0,0,0,0,0,0,0,0,0,0,0,
 10002 (00003)PHAST PLK-IMS   (00001)Phast Corp 0003   v3.12
       (PID=0:OID=0) Serial=0000000000000000
       Physical Address=NeuronID 0100417BD800
</pre></td></tr>
<tr><td><b>SHOW TCP</b></td><td>Displays a list of active TCP/IP connections.
Example:
<pre>
>SHOW TCP
 The following TCP connections exist(ed):
 1: IP=192.168.21.56:1042 Socket=0 (Dead)
 2: IP=192.168.21.56:1420 Socket=0 (Dead)
</pre></td></tr>
<tr><td><b>START LOG (ON|OFF)</b></td><td>Enables and disables the collection of startup log messages. Once enabled, the first x number of logs will be retained at startup for subsequent review via the "show start log" command. Use <code>SET LOG COUNT</code> (page 100) to set the number of log message that are retained.</td></tr>
<tr><td><b>TIME</b></td><td>Displays the current time on the Master.
Example:
<pre>
>TIME
 13:42:04
</pre></td></tr>
<tr><td><b>URL LIST <D:P:S&gt;</b></td><td>Displays the list of URL addresses programmed in the Master (or another system if specified).
Example:
<pre>
>URL LIST
    The following URLs exist in the URL connection list
  ->Entry 0-192.168.13.65:1319 IP=192.168.13.65 State=Connected
    Entry 1-192.168.13.200:1319 IP=192.168.13.200 State=Issue Connect
</pre></td></tr>
</table>

Terminal Commands (Cont.)	
Command	Description
USB LOG [front|back] [enable|disable]	Directs the Master logs to a USB flash media file. The log files are named with the current date and time. Syntax: `USB LOG [front|back] [enable|disable]`
ZEROCONF [ENABLE|DISABLE|STATUS]	Enable, disable or view the new Zeroconf client in the Master. When Zeroconf is enabled (default) the Master's web interface will be registered via Zeroconf and can be viewed through a Zeroconf browser plug-in such as Bonjour for IE.

ESC Pass Codes

There are 'escape' codes in the pass mode. These codes can switch the display mode or exit pass mode. The following 'escape' codes are defined.

Escape Pass Codes	
Command	Description
+ + ESC ESC	Exit Pass Mode: Typing a plus (shift =) followed by another plus followed by an ESC (the escape key) followed by another escape exits the pass mode. The Telnet session returns to "normal".
+ + ESC A	ASCII Display Mode: Typing a plus (shift =) followed by another plus followed by an ESC (the escape key) followed by an 'A' sets the display to ASCII mode. Any ASCII characters received by the device will be displayed by their ASCII symbol. Any non-ASCII characters will be displayed with a \ followed by two hex characters to indicate the characters hex value.
+ + ESC D	Decimal Display Mode: Typing a plus (shift =) followed by another plus followed by an ESC (the escape key) followed by a 'D' sets the display to decimal mode. Any characters received by the device will be displayed with a \ followed by numeric characters to indicate the characters decimal value.
+ + ESC H	Hex Display Mode: Typing a plus (shift =) followed by another plus followed by an ESC (the escape key) followed by an 'H' sets the display to hexadecimal mode. Any characters received by the device will be displayed with a \ followed by two hex characters to indicate the characters hex value.

Accessing the Security Configuration Options

Security configuration options are only available to Program Port connections (see the *Overview* section on page 90).

Note: *Refer to the SET SECURITY PROFILE* on page 101 *for information on setting Security Profiles.*

1. In the Terminal session, type **help security** to view the available security commands. Here is a listing of the security help:

```
---- These commands apply to the Security Manager and Database ----
logout                   Logout and close secure session
setup security           Access the security setup menus
```

Note: *The 'help security' and 'setup security' functions are only available via a direct Program Port connection. They are not available to Telnet sessions.*

2. Type **setup security** to access the *Setup Security* menu, shown below:

```
>setup security

---- These commands apply to the Security Manager and Database ----
 1) Set system security options for NetLinx Master
 2) Display system security options for NetLinx Master
 3) Add user
 4) Edit user
 5) Delete user
 6) Show the list of authorized users
 7) Add group
 8) Edit group
 9) Delete group
10) Show list of authorized groups
11) Set Telnet Timeout in seconds
12) Display Telnet Timeout in seconds
13) Enter LDAP security information
14) Test connection to the LDAP server
15) Make changes permanent by saving to flash
16) Reset Database
17) Display Database
Or <ENTER> to return to previous menu

Security Setup ->
```

3. The Setup Security menu shows a list of choices and a prompt. To select one of the listed choices, simply enter the number of the choice (**1** - **17**) at the prompt and press <Enter>.

Each option in the Setup Security menu displays a sub-menu specific to that option. The following subsections describe using each of the Setup Security menu options.

Note: *Changes made to the target Master from within the Terminal window are not reflected within the web browser, until the Master is rebooted and the web browser connection is refreshed. Any changes made to the Master, from within the web browser are instantly reflected within the Terminal session without the need to reboot.*

Setup Security Menu

The Setup Security menu is described below:

Setup Security Menu	
Command	Description
`1) Set system security options for NetLinx Master` See the *Security Options Menu* section on page 113 for descriptions of each menu item.	This selection will bring up the Security Options Menu that allows you to change the security options for the NetLinx Master. These are "global" options that enable rights given to users and groups. For instance, if you want to disable Telnet security for all users, you would simply go to this menu and disable Telnet security for the entire Master. This would allow any user, whether they have the rights to Telnet or not. These options can be thought of as options to turn on security for different features of the NetLinx Master.
`2) Display system security options for NetLinx Master`	This selection will display the current security options for the NetLinx Master.
`3) Add user`	This selection will prompt you for a name for the User you are adding. The User name must be a unique alpha-numeric string (4 - 20 characters). ***Note**: User and Group names are case sensitive.* After the User is added, you will be taken to the *Edit User* menu to setup the new User’s right (see page 114).
`4) Edit user`	This selection will prompt you select a User to edit properties for. Once you have selected the User you want to edit, it will take you to the *Edit User* menu so you can edit the User's rights (see page 114).
`5) Delete user`	This selection will prompt you select a user to delete.
`6) Show the list of authorized users`	This selection displays a list of users.
`7) Add group`	This selection will prompt you for a name for the Group you are adding. The Group name must be a unique alpha-numeric string (4 - 20 characters). ***Note**: User and Group names are case sensitive.* After the Group is added, you will be taken to the *Edit Group* menu to setup the new users right (see page 114).
`8) Edit group`	This selection will prompt you select a Group to edit properties for. Once you have selected the Group you want to edit, it will take you to the Edit Group Menu so you can edit the group's rights (see page 114).
`9) Delete group`	This selection will prompt you select a group to delete. A group can only be deleted if there are no users assigned to that group.
`10) Show list of authorized groups`	This selection displays a list of groups.
`11) Set Telnet Timeout in seconds`	This selection allows you to set the time a telnet session waits for a user to login. When a Telnet client connects to the NetLinx Master, it is prompted for a username. If the client does not enter a users name for the length of time set in this selection, the session will be closed by the NetLinx Master.
`12) Display Telnet Timeout in seconds`	This selection displays the time a telnet session waits for a user to login.
`13) Enter LDAP security information`	This selection prompts you to specify the LDAP URI. Once the URI is entered and enter is pressed, a prompt for the next LDAP parameter will be displayed, and so on until all LDAP parameters are entered. ***Note**: Options 3 - 10 (Add user, Edit user, Delete user, Show the list of authorized users, Add group, Edit group, Delete group, Show list of authorized groups) on the Security Setup menu are disabled when LDAP is enabled.*
`14) Test connection to LDAP server`	This selection initiates a bind to the BIND DN using the Search Password entered. • If the bind is successful, the message *Connection successful* is displayed. • If the server could not be reached or the bind is unsuccessful, the message *Could not connect to server* is displayed.

Setup Security Menu (Cont.)	
Command	Description
`15) Make changes permanent by saving to flash`	When changes are made to the security settings of the Master, they are initially only changed in RAM and are not automatically saved permanently into flash. This selection saved the current security settings into flash. Also, if you attempt to exit the Main Security Menu and the security settings have changed but not made permanent, you will be prompted to save the settings at that time.
`16) Reset Database (administrator only function)`	If a user has been given "administrator rights", this additional menu option is displayed. This selection will reset the security database to its Default Security Configuration settings, erasing all users and groups that were added. This is a permanent change and you will be asked to verify this before the database is reset. This function is only visible to administrators.
`17) Display Database (administrator only function)`	If a user has been given "administrator rights", this additional menu option is displayed. This selection will display the current security settings to the terminal (excluding user passwords). It also displays all users (minus passwords), their group assignment (if any) and their rights, as well as all groups and their rights. This function is only visible to administrators.

Enabling LDAP via the Program Port

1. Type setup security to access the Setup Security menu, shown below:

```
>setup security

---- These commands apply to the Security Manager and Database ----
 1) Set system security options for NetLinx Master
 2) Display system security options for NetLinx Master
 3) Add user
 4) Edit user
 5) Delete user
 6) Show the list of authorized users
 7) Add group
 8) Edit group
 9) Delete group
10) Show list of authorized groups
11) Set Telnet Timeout in seconds
12) Display Telnet Timeout in seconds
13) Enter LDAP security information
14) Test connection to the LDAP server
15) Make changes permanent by saving to flash
16) Reset Database
17) Display Database
Or <ENTER> to return to previous menu

Security Setup ->
```

2. To enable LDAP, enter **1** and press **Enter**. The following will be output to the screen:

```
NetLinx Master security is Enabled
Do you want to keep NetLinx Master security enabled? (y or n):
```

3. To proceed, enter **y** and press **enter**. The following menu will be displayed:

```
Select to change current security option

  1) Terminal (RS232) Security..........Enabled
  2) HTTP Security......................Enabled
  3) Telnet Security....................Enabled
  4) Configuration Security.............Enabled
  5) ICSP Security......................Disabled
  6) ICSP Encryption Required...........Disabled
  7) LDAP Security......................Disabled

Or <ENTER> to return to previous menu
```

4. To enable LDAP Security, enter **7** and press **Enter**. The same menu will be sent to the screen with LDAP Security set to Enabled. Press enter to return to the Security Setup menu.
5. When back to the Security Setup menu, enter **13** and press **Enter**.

   A prompt to enter the LDAP URI will be displayed. Once the URI is entered and enter is pressed, a prompt for the next LDAP parameter will be displayed.

   This will continue until all parameters are entered and then the Security Setup menu will be displayed again.
6. To save the security setup, enter **15** and press **Enter**.
7. To test the connection to the server enter **14** and press **Enter**.

   This test does a bind to the BIND DN using the Search Password entered. If the bind is successful, "**Connection successful**" is printed on the screen. If the server could not be reached or the bind is unsuccessful, "**Could not connect to server**" is printed on the screen.
8. Press **Enter** to return to the main menu.

***Note:** Options 3 - 10 (Add user, Edit user, Delete user, Show the list of authorized users, Add group, Edit group, Delete group, Show list of authorized groups) on the Security Setup menu are disabled when LDAP is enabled.*

Security Options Menu

Select "**Set system security**" from the Setup Security Menu to access the *Security Options* menu, described below:

Security Options Menu	
Command	Description

`1) Terminal (RS232) Security`
`(Enabled/Disabled)`
	This selection enables/disables Terminal Security. on the Program (RS232) Port.If *Terminal Security* is enabled, a user must have sufficient access rights to login to a Program Port terminal session.

`2) HTTP Security`
`(Enabled/Disabled)`
	This selection enables/disables HTTP (Web Server) Security. If *HTTP Security* is enabled, a user must have sufficient access rights to access the Master's WebConsole via a web browser.

`3) Telnet Security`
`(Enabled/Disabled)`
	This selection enables/disables Telnet Security. If *Telnet Security* is enabled, a user must have sufficient access rights to login to a Telnet terminal session.

`4) Configuration Security`
`(Enabled/Disabled)`
	This selection enables/disables configuration access rights for the Master. If *Configuration Security* is enabled, a user must have sufficient access rights to access the Setup Security menu (see page 111), and make changes to the Master's security parameters.

`5) ICSP Security`
`(Enabled/Disabled)`
	This selection enables/disables security of ICSP data being transmitted between the target Master and external AMX components (software and hardware such as TPD4 and a Modero Touch Panel).

`6) ICSP Encryption Required`
`(Enabled/Disabled)`
	This selection enables/disables the need to require encryption of the ICSP communicated data. If enabled:
	• All communicating AMX components must authenticate with a valid username and password before beginning communication with the Master.
	• All communication must be encrypted.

`7) LDAP Security`
`(Enabled/Disabled)`
	This selection enables/disables LDAP Security. Refer to *Appendix A: LDAP Implementation Details* on page 119 for details on LDAP Implementation.

Edit User Menu

The Edit User Menu is accessed whenever you enter the **Add user**, or **Edit user** selections from the Setup Security menu. The Edit User Menu options are described in the following table:

Edit User Menu

Command	Description
`1) Change User Password`	This selection prompts you to enter the new password (twice) for the user. Once the new password is entered, the user must use the new password from that point forward.
`2) Change Inherits From Group`	This selection will display the current group the user is assigned to (if any). It will then display a list of current groups and prompts you to select the new group.
`3) Add Directory Association`	This selection will display any current directory associations assigned to the user, and then will prompt you for a path for the new directory association.
`4) Delete Directory Association`	This selection will display any current directory associations assigned to the user, and then will prompt you to select the directory association you want to delete.
`5) List Directory Associations`	This selection will display any current Directory Associations assigned to the user.
`6) Change Access Rights`	This selection will display access the *Access Rights menu*, which allows you to set the rights assigned to the user. ***Note**: See the Access Rights Menu section (below) for descriptions of each menu item.*
`7) Display User Record Contents`	This selection will display the group the user is assigned to and the current Access Rights assigned to the user.

Edit Group Menu

The Edit Group Menu is accessed whenever you enter the **Add group**, or **Edit group** selections from the Setup Security menu. The Edit Group Menu options are described in the following table:

Edit Group Menu

Command	Description
`3) Add Directory Association`	This selection will display any current directory associations assigned to the group, and then will prompt you for a path for the new directory association.
`4) Delete Directory Association`	This selection will display any current directory associations assigned to the group, and then will prompt you to select the directory association you want to delete.
`5) List Directory Associations`	This selection will display any current Directory Associations assigned to the group.
`6) Change Access Rights`	This selection will display access the *Access Rights menu*, which allows you to set the rights assigned to the group. **Note**: See the *Access Rights Menu* section (below) for descriptions of each menu item.
`7) Display Access Rights`	This selection will display the current Access Rights assigned to the group.

Access Rights Menu

The Access Rights Menu is accessed whenever you select **Change Access Rights** (option **6**) from the Edit User menu, or **Change Access Rights** from the Edit Group menu. The options in this menu is described below:

Access Rights Menu	
Command	Description
`1) Terminal (RS232) Access (Enable/Disable)`	Enables/disables Terminal (RS232 Program port) Access. The account has sufficient access rights to login to a Terminal session if this option is enabled.
`2) Admin Change Password Access (Enable/Disable)`	Enables/disables Administrator Change Password Access. The account has sufficient access rights to change the administrator password if this option is enabled.
`3) FTP Access (Enable/Disable)`	Enables/disables FTP Access. The account has sufficient access rights to access the NetLinx Master's FTP Server if this option is enabled.
`4) HTTP Access (Enable/Disable)`	This selection enables/disables HTTP (Web Server) Access. The account has sufficient access rights to browse to the NetLinx Master with a Web Browser if this option is enabled.
`5) Telnet Access (Enable/Disable)`	This selection enables/disables Telnet Access. The account has sufficient access rights to login to a Telnet session if this option is enabled.
`6) Configuration Access (Enable/Disable)`	This selection enables/disables Configuration Access rights for the target Master. The account has sufficient access rights to access the Main Security Menu if this option is enabled.
`5) ICSP Security (Enabled/Disabled)`	This selection enables/disables ICSP communication access. The account has sufficient access rights to initiate ICSP data communication.
`6) ICSP Encryption Required (Enabled/Disabled)`	This selection enables/disables the need to require encryption of the ICSP communicated data. If enabled: • All communicating AMX components must authenticate with a valid username and password before beginning communication with the Master. • All communication must be encrypted.

Adding a Group

1. Type **7** and **<Enter>** at the Security Setup prompt (at the bottom of the Main Security Menu) to add a group account. A sample session response is:

```
The following groups are currently enrolled:
administrator

Enter name of new group:
```

2. Enter a name for the group. A group name is a valid character string (4 - 20 alpha-numeric characters) defining the group. This string is ***case sensitive***, and each group name must be unique.

3. Press <Enter> to display the Edit Group menu.

Edit Group Menu: Add Directory Association

1. At the **Edit Group** prompt, type **1** to add a new directory association.

   A *Directory Association* is a path that defines the directories and/or files that a particular user or group can access via the HTTP (Web) Server on the NetLinx Master. This character string can range from 1 to 128 alpha-numeric characters. This string is ***case sensitive***. This is the path to the file or directory you want to grant access. Access is limited to the user (i.e. doc:user) directory of the Master. All subdirectories of the user directory can be granted access.

   - A single '/' is sufficient to grant access to all files and directories in the user directory and it's sub-directory.
   - The '*' wildcard can also be added to enable access to all files.
   - All entries should start with a '/'.

   Here are some examples of valid entries:

Path	Notes
`/`	Enables access to the user directory and all files and subdirectories in the user directory.
`/*`	Enables access to the user directory and all files and subdirectories in the user directory.
`/user1`	If `user1` is a file in the user directory, only the file is granted access. If `user1` is a subdirectory of the user directory, all files in the `user1` and its sub-directories are granted access.
`/user1/`	`user1` is a subdirectory of the user directory. All files in the `user1` and its sub-directories are granted access.
`/Room1/iWeb ControlPages/*`	`/Room1/iWeb ControlPages` is a subdirectory and all files and its subdirectories are granted access.
`/results.txt`	`results.txt` is a file in the user directory and access is granted to that file.

   By default, all accounts that enable HTTP Access are given a `'/*'` Directory Association if no other Directory Association has been assigned to the account. When you are prompted to enter the path for a Directory Association, the NetLinx Master will attempt to validate the path. If the directory or file is not valid (i.e. it does not exist at the time you entered the path), the NetLinx Master will ask you whether you were intending to grant access to a file or directory. From the answer, it will enter the appropriate Directory Association. The NetLinx Master will not create the path if it is not valid. That must be done via another means, most commonly by using an FTP client and connecting to the FTP server on the NetLinx Master.

Default Security Configuration

By default, the NetLinx Master will create the following accounts, access rights, directory associations, and security options.

```
Account 1:             User Name: administrator
Password:              password
Group:                 administrator
Rights:                All
Directory Association: /*

Account 2:             User Name: NetLinx
Password:              password
Group:                 none
Rights:                FTP Access
Directory Association: none

Group 1:               Group: administrator
Rights:                All
Directory Association: /*

Security Options:      FTP Security Enabled
                       Admin Change Password Security Enabled
                       All other options disabled
```

- The ***administrator*** user account cannot be deleted or modified with the exception of its password. Only a user with "Change Admin Password Access" rights can change the administrator password.
- The ***NetLinx*** user account is created to be compatible with previous firmware versions.
- The ***administrator*** group account cannot be deleted or modified.
- The ***FTP Security*** and ***Admin Change Password Security*** are always enabled and cannot be disabled.

Note: *Refer to the SET SECURITY PROFILE* on page 101 *for information on setting Security Profiles.*

Telnet Diagnostics Commands

The following Telnet Diagnostics Commands provide visibility to remote Masters, in order to determine the current state of operations, and are provided as diagnostic/troubleshooting tools.

While these commands are available for any user to execute, their output is interpretable primarily by an AMX Technical Support Engineer.

Telnet Diagnostics Commands	
Command	Description
PHYSICAL STATUS	This command reports the current state of the Master's Status, Output and Input LEDs, in order to troubleshoot a remote Master. For example, if PHYSICAL STATUS indicates that the Input LED always shows '1' (or ON), it could indicate that the Master is being hammered by incoming events.
MSG STATS	This command collects messages statistics for the Interpreter over a 10 second period by calculating the number of event messages that have been processed. This can be useful as a debugging/diagnostics tool to determine if the NetLinx Interpreter is running and how many messages it's processing.

Logging Out of a Terminal Session

CAUTION!: *It is very important to execute the 'logout' command prior to disconnecting from a Master.*

Simply removing the RS-232 connector from the Program Port maintains your logged-in status until you either return to logout via a new session or reboot the target Master.

Notes on Specific Telnet/Terminal Clients

Telnet and terminal clients will have different behaviors in some situations. This section states some of the known anomalies.

Windows Client Programs

Anomalies occur when using a Windows™ client if you are not typing standard ASCII characters (i.e. using the keypad and the ALT key to enter decimal codes). Most programs will allow you to enter specific decimal codes by holding ALT and using keypad numbers.

For example, hold ALT, hit the keypad 1, then hit keypad 0, then release ALT. The standard line feed code is entered (decimal 10). Windows will perform an ANSI to OEM conversion on some codes entered this way because of the way Windows handles languages and code pages.

The following codes are known to be altered, but others may be affected depending on the computer's setup.

Characters 15, 21, 22, and any characters above 127.

This affects both Windows Telnet and Terminal programs.

Linux Telnet Client

The Linux Telnet client has three anomalies that are known at this time:

- A null (\00) character is sent after a carriage return.
- If an ALT 255 is entered, two 255 characters are sent (per the Telnet RAFT).
- If the code to go back to command mode is entered (ALT 29 which is ^]), the character is not sent, but Telnet command mode is entered.

Appendix A: LDAP Implementation Details

Overview

The process of verifying credentials and obtaining user authorization is designed to support most organizations requirements for 'least privilege'. The account used to search LDAP to provide user objects for authentication never needs access to user information. Authorization lookups are performed as the authenticated user and as such, no elevated permission is required. Please refer to RFC 2256, RFC 2798, and RFC 4519.

Assumptions and Prerequisites

Assumptions made about the LDAP implementation or environment in which the AMX client will participate include:

1. Must support simple authentication (for example, NetLinx Masters do not support *Kerberos* or *SASL*).
2. The account setup for a bind DN must have search capability along with the necessary permissions to read the 'uid', 'cn', 'member' and 'objectclass' attributes.
3. When a search is performed to find a DN with the specified user ID, a search must return one and only one object if the user exists. No object will be returned if an account does not exist for that user ID.
4. An account is considered valid if a user can authenticate/bind. No other attributes are considered during the authentication process.
5. AMX LDAP implementation supports both encrypted and un-encrypted connections using SSL.
6. When a person authenticates, that account must have access to all the attributes defined by RFC 2798 with the following exception:

   User passwords are not necessarily accessible for anything except to perform a bind to the directory (for example, this attribute may not be directly available to the user).
7. When a person authenticates, that account must have the ability to search for the groups of which that account is a member (for example, the account is able to perform a search with a filter which contains 'member=' followed by the DN of the authenticated user. If exceptions exists, those groups cannot/will not be necessary for AMX client security decisions.
8. When a person authenticates, that account must have access to "cn" attributes for all groups of which it is a member.
9. Group membership for users will be defined by the *GroupOfNames* object class. *GroupOfUniqueNames* is not supported due to ambiguities associated with implementations which use unique IDs appended to membership DNs.
10. When performing searches for group membership, no restrictions exist which would the restrict returning the full list of objects for which the user is a member with the possible exception of reasonable response timeouts. AMX LDAP implementation does not support paged search results.
11. AMX LDAP implementation does not support following referrals.

AMX LDAP Client Authentication Sequence

An example of the operation of the AMX client, using the example LDAP directory tree in the server section of this document, is presented next in a step-by-step breakdown. *DallasUser1* will be used for this example.

Client Setup:

LDAP Enabled: **yes**

LDAP URI: **ldaps://myLDAPServer01: 636**

LDAP BASE DN: **dc=example,dc=com**

BIND DN: **uid=amxBindAccount,ou=people,dc=example,dc=com**

User Query Attr: **uid**

Search Password: **secret**

1. *DallasUser1* initiates a HTTP session with the master and is prompted for a user name and password.
2. *DallasUser1* enters user name: **DallasUser1** and his/her password: **DallasUser1Pswd**.

3. The client connects to the LDAP server and starts a bind operation with the BIND DN, **uid=amxBindAccount,ou=people,dc=example,dc=com**, and the Search Password, **secret**.
4. The password, *secret*, is then compared by the server to the value of the userPassword attribute for the record **uid=amxBindAccount,ou=people,dc=example,dc=com**.

   If this step is successful, the bind is successful and the client is logged in.
5. If the bind is successful, the client then performs a search with the filter **(&(objectclass=person)(uid=DallasUser1)**).

   The *objectclass=person* portion of the filter is hard coded in the client firmware.

   The *uid=DallasUser1* portion of the filter is formed from the configured parameter *User Query Attr* and the user name entered when logging in.

   Since the *User Query Attr* is required to be unique in the search base LDAP BASE DN, the search should return either 0 or 1 record.

   If one record is found, the DN of the record is returned. In this example, the DN **uid=DallasUser1,ou=people,ou=Dallas,dc=example,dc=com** is returned.
6. The client then unbinds as the user **uid=amxBindAccount,ou=people,dc=example,dc=com**.
7. If a record is found that matches, the client then attempts to bind as this DN using the password the user enters to initiate the session.

   In this example the DN **uid=DallasUser1,ou=people,ou=Dallas,dc=example,dc=com** and the password **DallasUser1Pswd** would be used for this bind.
8. The server compares the user supplied password with the value of the *userPassword* attribute of **uid=DallasUser1,ou=people,ou=Dallas,dc=example,dc=com**.

   If this match is successful, the bind is successful and the client is logged in.
9. If the bind is successful, the client then performs another search using the filter (member=DN returned from the first search) specifying that the *commonName* attribute of matching entries should be returned.

   In this example, the filter is **member=uid=DallasUser1,ou=people,ou=Dallas,dc=example,dc=com**.

   Since *DallasUser1* is listed as a member of the groupOfNames objectclass

   dn: cn=master01Admin,ou=groups,ou=Dallas,dc=example,dc=com

   and

   dn: cn=master01User,ou=groups,ou=Dallas,dc=example,dc=com,

   the server will return the *commonName* attributes **master01Admin** and **master01User**.

   The client then unbinds as this user and exits.

Note: *The AMX LDAP client configuration parameters are located on the System Security Details page under the System Security Settings link. See the System Security - System Level* section on page 24*; the LDAP configuration options are described on page 34.*

Example - Setting Up User's Access Rights

In order to give AMX equipment users access rights to the Master, group memberships for users will be defined by the *GroupOfNames* object class (refer to LDAP RFC4519). Two records need to be created in the database:

- One that represents users with administrative privileges (Admin Change Password Access, Terminal (RS232) Access, FTP Access, HTTP Access, Telnet Access, Configuration, ICSPConnectivity, and EncryptICSP Connection).
- Another that represents users with user privileges (HTTP Access). The DNs of the AMX equipment users will be listed under the appropriate GroupOfNames object class as a member attribute.

Administrator Access Example

Administrator Access	
LDAP Server Configuration	Master Configuration
Example: **dn**: cn=master01Admin,ou=groups,ou=Dallas, dc=example,dc=com **objectClass**: groupOfNames **objectClass**: top **cn**: master01Admin **member**: uid=DallasAdminUser1,ou=people, ou=Dallas,dc=example,dc=com **member**: uid=ICSPUser,ou=people, ou=Dallas,dc=example,dc=com	On the *System Security Details* page, enter the Administrator groupOfNames cn. *Example*: **Admin groupOfNames cn**: master01Admin

User Access Example

User Access	
LDAP Server Configuration	Master Configuration
Example: **dn**: cn=master01User,ou=groups, ou=Dallas,dc=example,dc=com **objectClass**: groupOfNames **objectClass**: top **cn**: master01User **member**: uid=DallasUser1,ou=people, ou=Dallas,dc=example,dc=com **member**: uid=DallasUser2,ou=people, ou=Dallas,dc=example,dc=com	On the *System Security Details* page, enter the User groupOfNames cn. *Example*: **User groupOfNames cn**: master01User

Note: *If the DN of a user is in both the administrator groupOfNames and the user groupOfNames, the administrative privileges take precedence over user privileges.*

ICSP Connectivity Security Example

If ICSP connectivity is enabled, a valid user name and password is required to communicate with the NetLinx Master via an ICSP connection (TCP/IP, UDP/IP and RS-232). This is used with communication amongst various AMX hardware and software components.

User Access	
LDAP Server Configuration	Master Configuration
An ICSP user should be configured for a specific Master and should be set up as a normal user. Example: **dn**: uid=ICSPUser,ou=people,ou=Dallas, dc=example,dc=com **objectClass**: inetOrgPerson **objectClass**: organizationalPerson **objectClass**: person **objectClass**: top **cn**: ICSP User **sn**: User **uid**: ICSPUser **userPassword**: password ***Note**: The DN of this user must be added as a member to the administrator groupOfNames objectClass on the server.*	1) On the *System Security Details* page, disable LDAP by clearing the *LDAP Enabled* check box and disable ICSP Connectivity by clearing the *ICSP Connectivity* check box. 2) Click the User level tab and navigate to the User Security Details page. 3) Create a new user by clicking *Add New User.* 4) Enter the User name and password as set up on the LDAP server (for example: ICSPUser and password). 5) Set all Access privileges. 6) Click the *Accept* button to complete adding the new user. 7) Return to the *System Security Details* page, and enter the common name (cn) of the groupOfNames objectClass that contains the member DN of the ICSP user that was just configured, and enable ICSP Connectivity, Encrypt ICSP Connection and LDAP by clicking on the appropriate checkboxes. ***Note**: If there is a mismatch with the user name or password, the AMX hardware or software component will not be allowed access. If there is a mismatch with the access privileges, the master will use the privileges value stored on the server.*

Appendix B: SMTP Support

Overview

NetLinx Integrated Controllers (Masters) have built-in support for transmission or email via an SMTP server. NetLinx Master support includes the configuration of a single outbound SMTP server and the subsequent transmission of individual emails via the configured server.

SMTP Server Configuration

The SMTP Server is configured by specifying a set of server properties. SMTP server properties once set are persistent on the master until they are reset to a different value. SMTP server properties include the server IP address or URL, the SMTP IP port number for connecting to the server, any username and password that is required for connecting with the server, the "from" address that will be associated with all outgoing messages and finally a flag indicating if the server must support TLS authentication security in order to establish a connection. Properties are set and read using two built-in NetLinx functions:

```
SMTP_SERVER_CONFIG_SET(CONSTANT CHAR cfgName[], CONSTANT CHAR cfgValue[])
```

Sets a server configuration parameter.   These configuration settings are general mail server settings and thus apply to all emails. Settings are saved to the configuration database & thus are static upon reboot.

cfgName is the server property name that is being set. Acceptable values are

- *ADDRESS* - SMTP server name, such as "mail.amx.com". The maximum number of characters allowed for email destination is 127.
- *PORT* - SMTP server port, such as "25" or "0". 0 means "use the best default port" which would imply using 25 which is the SMTP well-known port.
- *USERNAME* - User name to offer for authentication. If user name length is set to 0, authentication is not attempted.
- *PASSWORD* - Password to offer for authentication. If password length is set to 0, authentication is still attempted but simply uses a zero-length password.
- *FROM* - Mail address to populate to the 'Mail-From:' field in outgoing emails.
- *REQUIRE_TLS* - SMTP server must support TLS in order to establish a connection. Valid values are 'TRUE' or 'FALSE'

cfgValue is the value to associate for a setting property.

```
char[] SMTP_SERVER_CONFIG_GET (CONSTANT CHAR cfgName[])
```

Queries a server configuration property. Returns the config property value.

cfgName is the server property name that is being retrieved. Acceptable values are a subset of the settable properties (username & password query are disabled as a security precaution). No return value

- *ADDRESS* - SMTP server name, such as "mail.amx.com". The maximum number of characters allowed for email destination is 127.
- *PORT* - SMTP server port, such as "25" or "0". 0 means "use the best default port" which would imply using 25 which is the SMTP well-known port.
- '*FROM* - Mail address populated to the 'Mail-From:' field in outgoing emails.
- *REQUIRE_TLS* - SMTP server must support TLS in order to establish a connection. Valid values are 'TRUE' or 'FALSE'

The **NetLinx .axi** file has the following built in constants to ease configuration:

```
CHAR SMTP_ADDRESS[] = 'ADDRESS';
CHAR SMTP_PORT_NUMBER[] = 'PORT';
CHAR SMTP_USERNAME[] = 'USERNAME';
CHAR SMTP_PASSWORD[] = 'PASSWORD';
CHAR SMTP_REQUIRE_TLS[] = 'REQUIRE_TLS';
CHAR SMTP_FROM[] = 'FROM';
CHAR NULL_STR[] = '';
CHAR SMTP_TLS_TRUE[] = 'TRUE';
CHAR SMTP_TLS_FALSE[] = 'FALSE';
```

Example server configuration:

```
SMTP_SERVER_CONFIG_SET(SMTP_ADDRESS,'mail.mymailserver.com')
SMTP_SERVER_CONFIG_SET(SMTP_PORT_NUMBER,'25')
SMTP_SERVER_CONFIG_SET(SMTP_USERNAME,'myAccountUsername')
SMTP_SERVER_CONFIG_SET(SMTP_PASSWORD,'myAccountPassword')
SMTP_SERVER_CONFIG_SET(SMTP_REQUIRE_TLS, SMTP_TLS_TRUE)
SMTP_SERVER_CONFIG_SET(SMTP_FROM,'John Doe')
```

Sending Mail

Sending mail is accomplished with the use of the Master's built-in Mail Service. An outbound mail is handed to the Mail Service via the following built-in NetLinx function:

```
sinteger SMTP_SEND (DEV responseDPS, CONSTANT CHAR toAddress[], CONSTANT CHAR mailSubject[], CONSTANT
CHAR mailBody[], CONSTANT CHAR textAttachment[])
```

where:

- *responseDPS* - The DPS address to return asynchronous send status. Ex. 0:3:0
- *toAddress* - The email address of destination. Ex. `john.doe@amx.com`.

  Note that the NetLinx mail service supports up to eight recipient address (semi-colon delimited). These are "To" addresses only (not "Cc" or "Bcc" addresses.)

  The maximum number of characters allowed for email destination is 127.
- *mailSubject* - The email subject line.
- *mailBody* - The email body text.
- *textAttachment* - A text filename to attach to the email (optional argument). Filenames must be 256 characters or less, and file size must be under 65536 bytes. When no attachment is included textAttachment should be set to `NULL_STR`.

`SMTP_SEND` returns a signed integer.

- If the return value is negative (<0) that is an indication there was a failure in handing the message off to the mail service, most likely due to an invalid argument supplied to the `SMTP_SEND` call.
- If the return value is positive (>0) then the value is the index associated with the mail being sent.
- Mail sends are asynchronous to the normal processing of the NetLinx application.
- When `SMTP_SEND` is called and the mail is posted to the internal Mail Service, the NetLinx application will continue executing the code following the `SMTP_SEND`.
- The failed send status will be returned via an `ONERROR DATA_EVENT` for the *responseDPS* specified in the `SMTP_SEND` call with `DATA.NUMBER` set to the error code and `DATA.TEXT` set to the mail identifier returned from the `SMTP_SEND` call.

Example `SMTP_SEND`:

```
DEFINE_DEVICE
MAIL_SERVICE=0:3:0

DEFINE_VARIABLE
SINTEGER MAIL_IDX

…
MAIL_IDX = SMTP_SEND(MAIL_SERVICE,'jdoe@somemail.com','Mail Subj','Mail Body', NULL_STR)
IF (MAIL_IDX < 0)
{
     // FAILED TO SEND MAIL
}
…
DATA_EVEN [MAIL_SERVICE]
{
     ONERROR:
     {
          // AN ERROR OCCURRED
          LOG_ERROR("MAIL SEND FAILURE - IDX=',DATA.TEXT,' ERROR=',ITOA(DATA.NUMBER))
     }
}
```

The possible error codes are:

```
MALFORMED DATA = 1;
NOT ENOUGH MEMORY = 2;
SERVER UNREACHABLE = 3;
AUTHENTICATION FAILURE = 4;
SMTP PROTOCOL ERROR = 5;
```

Appendix C: Clock Manager NetLinx Programming API

Types/Constants

The NetLinx.axi file that ships with NetLinx Studio includes the following types/constants:

```
(*-----------------------------------------------------------------------------*)
(* Added v1.28, Clock Manager Time Offset Structure *)
(*-----------------------------------------------------------------------------*)
STRUCTURE CLKMGR_TIMEOFFSET_STRUCT
{
  INTEGER     HOURS;
  INTEGER     MINUTES;
  INTEGER     SECONDS;
}

(*-----------------------------------------------------------------------------*)
(* Added v1.28, Clock Manager Time Server Entry Structure *)
(*-----------------------------------------------------------------------------*)
STRUCTURE CLKMGR_TIMESERVER_STRUCT
{
  CHAR     IS_SELECTED;               (* TRUE/FALSE *)
  CHAR     IS_USER_DEFINED;           (* TRUE/FALSE *)
  CHAR     IP_ADDRESS_STRING[48];     (* Allow enough room for IPv6 in the future *)
  CHAR     URL_STRING[32];            (* Example: time.organization.net *)
  CHAR     LOCATION_STRING[32];       (* Example: Boulder, Colorado, US *)
}

(* Added v1.28, Clock Manager *)
INTEGER CLKMGR_MODE_NETWORK    = $01; (* Used to enable Clock Manager Functionality *)
INTEGER CLKMGR_MODE_STANDALONE = $02; (* Use a free-running clock - legacy behavior.*)
```

Library Calls

The NetLinx.axi file that ships with NetLinx Studio includes the following Clock Manager-specific library calls:

NetLinx.axi - Library Calls	
CLKMGR_IS_NETWORK_SOURCED()	Returns FALSE/0 or TRUE/1 (default = FALSE/0)
CLKMGR_SET_CLK_SOURCE (CONSTANT INTEGER MODE)	Can be set to CLKMGR_MODE_NETWORK or CLK-MGR_MODE_STANDALONE.
CLKMGR_IS_DAYLIGHTSAVINGS_ON()	Returns FALSE/0 or TRUE/1 (default = FALSE/0).
CLKMGR_SET_DAYLIGHTSAVINGS_MODE (CONSTANT INTEGER ONOFF)	Can be set to ON/TRUE or OFF/FALSE.
CLKMGR_GET_TIMEZONE()	Returns Timezone as a string in the format: UTC[+|-]HH:MM
CLKMGR_SET_TIMEZONE (CONSTANT CHAR TIMEZONE[])	Input string must have the correct format: UTC[+|-]HH:MM
CLKMGR_GET_RESYNC_PERIOD()	Returns the Clock Manager's re-sync period in minutes (default = 60). This setting has no effect if the Clock Manager mode is set to STANDALONE.
CLKMGR_SET_RESYNC_PERIOD (CONSTANT INTEGER PERIOD)	Sets the re-sync period to the specified minute value. The upper bound is 480 minutes (i.e., 8 hours).
CLKMGR_GET_DAYLIGHTSAVINGS_OFFSET (CLKMGR_TIMEOFFSET_STRUCT T)	Populates the TIMEOFFSET structure with the current Daylight Savings Offset configured. The function returns a negative SLONG value if it encounters an error.
CLKMGR_SET_DAYLIGHTSAVINGS_OFFSET (CONSTANT CLKMGR_TIMEOFFSET_STRUCT T)	Sets the Daylight Savings Offset to the specified value.
CLKMGR_GET_ACTIVE_TIMESERVER (CLKMGR_TIMESERVER_STRUCT T)	Populates the TIMESERVER structure with the currently active time server's data. The function returns a negative SLONG value if it encounters an error.

NetLinx.axi - Library Calls (Cont.)	
CLKMGR_SET_ACTIVE_TIMESERVER (CONSTANT CHAR IP[])	Sets the time server entry that has the matching IP-ADDRESS to the IP parameter as the active time server entry.
CLKMGR_GET_TIMESERVERS (CLKMGR_TIMESERVER_STRUCT T[])	Populates the currently configured time server entries from the Clock Manager into the specified TIMESERVER array. The function returns a negative SLONG value if it encounters an error, otherwise the return value is set to the number of records populated into the CLK-MGR_-TIMESERVER_STRUCT array.
CLKMGR_ADD_USERDEFINED_TIMESERVER (CONSTANT CHAR IP[], CONSTANT CHAR URL[], CONSTANT CHAR LOCATION[])	Adds a user-defined time server entry.
CLKMGR_DELETE_USERDEFINED_ TIMESERVER(CONSTANT CHAR IP[])	Deletes the user-defined entry that has its IP-ADDRESS matching the parameter.
CLKMGR_GET_START_ DAYLIGHTSAVINGS_RULE()	Gets a string representation of when Daylight Savings is supposed to START. The Fixed-Date rules have the form: "fixed:DAY,MONTH,HH:MM:SS" with all fields as numeric except for the word "fixed". The Occurrence-Of-Day rules have the form: "occurence:OCCURENCE,DAY-OF-WEEK,MONTH,HH:MM:SS" with all fields as numeric except for the word "occurence". • OCCURANCE range = 1-5 ’5’ indicates the 'LAST' occurrence of a particular day of the month. • DAY-OF-WEEK translates as: 1=Sunday 2=Monday 3=Tuesday 4=Wednsday 5=Thursday 6=Friday 7=Saturday Examples: "fixed:5,10,16:00:00" = October 5, at 4:00PM). "occurence:5,1,10,02:00:00" = last Sunday in October, at 2:00AM).
CLKMGR_SET_START_DAYLIGHTSAVINGS_RULE (CONSTANT CHAR RECORD[])	Sets the START Daylight Savings rule to the specified string which *must* be in either the Fixed-Date format or the Occurence-Of-Day format. The function returns a negative SLONG value if it encounters an error. The Fixed-Date rules have the form: "fixed:DAY,MONTH,HH:MM:SS" with all fields as numeric except for the word "fixed". The Occurrence-Of-Day rules have the form: "occurence:OCCURENCE,DAY-OF-WEEK,MONTH,HH:MM:SS" with all fields as numeric except for the word "occurence". • OCCURANCE range = 1-5 ’5’ indicates the 'LAST' occurrence of a particular day of the month. • DAY-OF-WEEK translates as: 1=Sunday 2=Monday 3=Tuesday 4=Wednsday 5=Thursday 6=Friday 7=Saturday Examples: "fixed:5,10,16:00:00" = October 5, at 4:00PM). "occurence:5,1,10,02:00:00" = last Sunday in October, at 2:00AM).

NetLinx.axi - Library Calls (Cont.)	
CLKMGR_GET_END_DAYLIGHTSAVINGS_RULE()	Gets a string representation of when Daylight Savings is supposed to END. The Fixed-Date rules have the form: "fixed:DAY,MONTH,HH:MM:SS" with all fields as numeric except for the word "fixed". The Occurrence-Of-Day rules have the form: "occurence:OCCURENCE,DAY-OF-WEEK,MONTH,HH:MM:SS" with all fields as numeric except for the word "occurence". • OCCURANCE range = 1-5 ’5’ indicates the 'LAST' occurrence of a particular day of the month. • DAY-OF-WEEK translates as: 1=Sunday 2=Monday 3=Tuesday 4=Wednsday 5=Thursday 6=Friday 7=Saturday Examples: "fixed:5,10,16:00:00" = October 5, at 4:00PM). "occurence:5,1,10,02:00:00" = last Sunday in October, at 2:00AM).
CLKMGR_SET_END_DAYLIGHTSAVINGS_RULE (CONSTANT CHAR RECORD[])	Sets the END Daylight Savings rule to the specified string which MUST be in either the Fixed-Date format or the Occurence-Of-Day format. The function returns a negative SLONG value if it encounters an error. The Fixed-Date rules have the form: "fixed:DAY,MONTH,HH:MM:SS" with all fields as numeric except for the word "fixed". The Occurrence-Of-Day rules have the form: "occurence:OCCURENCE,DAY-OF-WEEK,MONTH,HH:MM:SS" with all fields as numeric except for the word "occurence". • OCCURANCE range = 1-5 ’5’ indicates the 'LAST' occurrence of a particular day of the month. • DAY-OF-WEEK translates as: 1=Sunday 2=Monday 3=Tuesday 4=Wednsday 5=Thursday 6=Friday 7=Saturday Examples: "fixed:5,10,16:00:00" = October 5, at 4:00PM). "occurence:5,1,10,02:00:00" = last Sunday in October, at 2:00AM).

Increase Your Revenue
through education + knowledge

In the ever-changing AV industry, continual education is key to success. AMX University is dedicated to ensuring that you have the opportunity to gather the information and experience you need to deliver strong AMX solutions. Plus, AMX courses also help you earn CEDIA, NSCA, InfoComm, and AMX continuing education units (CEUs).

Visit AMX University online for 24/7/365 access to:
- *Schedules and registration for any AMX University course*
- *Travel and hotel information*
- *Your individual certification requirements and progress*